FINAL PROJECT REPORT

PRIVACY IN THE SMART GRID: AN INFORMATION FLOW ANALYSIS

Prepared for CIEE By:

University of California, Berkeley

Project Manager: Deirdre Mulligan

Authors: Deirdre K. Mulligan, Longhao Wang, Aaron J. Burstein
Date: March, 2011

A CIEE Report

ACKNOWLEDGEMENTS

The authors wish to thank Gaymond Yee for his guidance, support, and responsiveness. We also thank Ron Hofmann and Roger Levy for sharing their valuable insights on a broad array of technical and business-related aspects of California's Smart Grid policies and for their comments on a draft of this report.

We would like to thank Joseph Lorenzo Hall, Bob Lockhart, Jennifer Lynch, Maryanne McCormick, Jennifer Urban, and Steve Weissman for helpful comments on a draft of this report. We also thank Jim Dempsey and Ari Schwartz for helpful discussions during the drafting of public comments that helped to inform this report. Thanks to Nick Doty, Jess Hemerly, and Kimra McPherson for assistance with the final edit.

PREFACE

The California Energy Commission Public Interest Energy Research (PIER) Program supports public interest energy research and development that will help improve the quality of life in California by bringing environmentally safe, affordable, and reliable energy services and products to the marketplace.

The PIER Program conducts public interest research, development, and demonstration (RD&D) projects to benefit California.

The PIER Program strives to conduct the most promising public interest energy research by partnering with RD&D entities, including individuals, businesses, utilities, and public or private research institutions.

PIER funding efforts are focused on the following RD&D program areas:

- Buildings End-Use Energy Efficiency
- Energy Innovations Small Grants
- Energy-Related Environmental Research
- Energy Systems Integration
- Environmentally Preferred Advanced Generation
- Industrial/Agricultural/Water End-Use Energy Efficiency
- Renewable Energy Technologies
- Transportation

Privacy in the Smart Grid: An Information Flow Analysis is the final report for the Privacy Issues in the Smart Grid project (contract number 500-01-043), conducted by the University of California, Berkeley School of Information. The information from this project contributes to PIER's Demand Response Enabling Technology Development Program.

For more information about the PIER Program, please visit the Energy Commission's website at www.energy.ca.gov/research/ or contact the Energy Commission at 916-654-4878.

ABSTRACT

Smart meters, smart devices, and gateways allowing automated control of in-home devices are linchpins in an ambitious vision of creating a Smart Grid that will increase efficiency, improve grid resilience and reliability, and reduce peak demand. The collection, retention, and use of detailed usage data, however, put individual privacy at risk. Utilities, commercial third parties, law enforcement agents, parties in civil litigation, and criminals can discern from usage patterns whether a home is occupied and, to some extent, what is occurring inside.

The two-way communication channel also supports remote control of appliances to manage load. The ability to remotely control in-home electricity use through controlling devices within the home raises new security and privacy issues.

The Smart Grid is developing rapidly. Smart Grid systems are generating, collecting, and processing information that is far more voluminous and revealing than traditional meter data. Decisions about how best to address the emerging privacy issues—whether through technical design, best practices, or regulation—lag behind development of the system infrastructure.

This report documents the Smart Grid information flows and considers the laws and agencies that protect, or could protect, privacy in this new technological landscape. Legal sources of privacy protection are highly varied, ranging from state public utilities commissions to the Federal Trade Commission. The extent and level of privacy protection depends critically upon the route information takes from source to destination. Though state utilities regulators have traditionally played a strong role in protecting customer privacy, like other regulators, their jurisdiction is limited. Changes in the architecture of the energy grid that create new data flows and empower new players to handle data threaten to render some privacy provisions obsolete and others ineffective. Given the proliferation of data, industry players, and usage models, new laws and privacy-protecting technical designs are necessary to afford privacy, comparable to that enjoyed today, to users of tomorrow's energy network. Considering privacy upfront, rather than after technologies are deployed, will help build privacy protections into the Smart Grid while supporting other energy policy goals.

Keywords: Public Interest Energy Research program, PIER, Smart Grid, smart meter, privacy, surveillance cybersecurity, interoperability, energy usage information, home area network, HAN, energy management system, EMS

Please use the following citation for this report:

Mulligan, Deirdre K., Wang, Longhao, and Burstein, Aaron J.. University of California, Berkeley. 2010. ***Privacy in the Smart Grid: An Information Flow Analysis.*** California Institute for Energy and Environment. Final Project Report.

TABLE OF CONTENTS

Acknowledgements ..... **ii**

PREFACE ..... **iii**

ABSTRACT ..... **iv**

TABLE OF CONTENTS ..... **v**

LIST OF FIGURES ..... **vii**

EXECUTIVE SUMMARY **1**

Introduction 1

Purpose 2

Project Outcomes 2

Conclusions 2

Recommendations 3

CHAPTER 1: Introduction **5**

1.1 Background 5

1.2 Project Approach 10

1.3 Scope and Organization of this Report 11

CHAPTER 2: Policy Frameworks: Smart Grid and Information Privacy **12**

2.1 Federal Smart Grid Policy 12

2.2 California Smart Grid Policy 13

2.3 Relating Smart Grid Architecture to Information Privacy Frameworks 16

CHAPTER 3: Privacy Risks in Smart Grid Information Flows **19**

3.1 Meter Data and Energy Usage Information Privacy Risks 19

3.1.1 Meter Data Sent from Meter to Utility 19

3.1.2 Energy Usage Information Collected by a Customer-Owned Metering Device 25

3.1.3 Third Party Access to Energy Usage Information Held by Utilities 28

3.1.4 Energy Usage Information from Smart Meter to HAN 37

3.2 Load Management Information Privacy Risks 42

3.2.1 Direct Utility-HAN Device Communication 42

3.2.2 Customer-Owned Energy Management System (EMS) 48

3.2.3 Third-Party Energy Management Systems 51

3.3 Cross-Cutting Privacy Issues in Plug-In Electric Vehicles 53
CHAPTER 4: Conclusions and Recommendations 57
4.1 Conclusions 57
4.2 Recommendations 57
4.3 Benefits to California 59
GLOSSARY 60
APPENDIX A: 63
CPUC Decisions Approving Residential AMI Investments 63
APPENDIX B: 65
Major HAN Communication Protocols 65

LIST OF FIGURES

Figure 1: Meter data flow from electromechanical meter to utility. 7
Figure 2: Meter data flow between smart meter and utility 20
Figure 3: Meter data collected by customer-owned meter 27
Figure 4: Energy usage information flow patterns involving third parties 30
Figure 5: Energy usage information flow on the home area network 39
Figure 6: Utility-to-HAN load management information 44
Figure 7: Load management information flows with a customer-owned EMS 50
Figure 8: Load management information flows with a third-party EMS 53
Figure 9. Information flows from plug-in electric vehicle charging 55

EXECUTIVE SUMMARY

Introduction

The Smart Grid, by incorporating information technology into the electric grid, offers the promise of advancing several important energy policy goals: increasing efficiency, reducing peak demand, improving grid reliability and resiliency, and incorporating distributed and variable energy sources.

This same information technology, however, also creates privacy risks to residential electricity customers. Electricity meters are becoming information gateways that provide fine-grained details about home energy use. Whereas most customers are familiar with monthly meter readings, smart meters will provide hundreds of data points per month. These records alone can reveal a significant level of detail about what occurs within customers' homes—when they are awake or asleep, or when they are at home or away. The prospect of utilities or third parties controlling devices in customers' homes introduces a different kind of privacy issue: a remote entity (utility or third party) altering the behavior of appliances and other devices work inside customers' homes. This would represent a significant opening of the physical boundaries of the home.

Smart Grid data will not be confined to utilities. The California Public Utilities Commission (CPUC) is requiring utilities to honor customers' requests to make energy usage data available to third parties. Today, these third parties are not covered by the same regulatory or legislative privacy rules as utilities. The CPUC has also approved investments in devices, to be embedded in smart meters, that will allow utilities and third parties to communicate with appliances in customers' homes. Moreover, customers can purchase their own metering and control devices, opening the possibility that customers will rely on entities other than utilities to provide them with information about their energy use and to control their devices.

Unique privacy and security issues arise from the use of this two-way communication channel by utilities (or third parties) to control smart devices in customers' homes. Individuals will have incentives—financial or otherwise—to permit such remote control. This breaches a physical barrier that has protected individual decisions about how and when to use devices in the privacy of the home.

Decisions about Smart Grid architecture will have profound implications for privacy. These design choices will affect whether information leaves the home, where it goes, and who can access it. These same decisions will also influence grid cybersecurity. Finally, these architectural choices may profoundly influence how and where innovation and competition occur by expanding or limiting the freedom end-users have to choose the devices and services they use to connect their homes with the Smart Grid.

These issues transcend the geographic boundaries that dominate utility regulation and require immediate and ongoing attention at the national level. To be sure, utilities regulators have important roles to play in stating clear requirements for Smart Grid privacy, as well as protecting individuals by creating rules to govern data collection and use and to ensure that individuals have meaningful choices about whether and how to participate in Smart Grid initiatives. Supporting these policy goals through Smart Grid architecture would likely be done most efficiently at the national level. Unfortunately, the main source of federal guidance on

Smart Grid data privacy takes it as a given that Smart Grid systems will generate, store, and use large amounts of sensitive information; and the guidance is largely limited to internal policy and data processing suggestions for utilities and other private firms.[1]

Purpose

This project serves the California Energy Commission Public Interest Energy Research Program goal of promoting demand response by assessing privacy risks in Smart Grid technologies that are in use, or may soon be in use, in the state. This report also provides insight into how and where to address these risks.

Project Outcomes

This project has met the objectives of comprehensively reviewing both Smart Grid technologies—particularly those that are relevant to residential customers—and privacy laws and regulations, and interacting with relevant experts to identify threats that the Smart Grid presents to individual privacy. Smart Grid technologies in or near deployment support a wide variety of electricity usage data flows, and the legal protections for the privacy interests in that data vary considerably depending on who obtains the data, and how. The report's detailed analysis of eight salient information flows points to technical design choices that could mitigate privacy risks. This analysis also highlights gaps and inconsistencies in legal protections for Smart Grid data privacy.

Conclusions

Though the Smart Grid is in its early stages, its potential to lead to privacy intrusions by commercial entities, law enforcement agencies, parties to civil litigation, and criminals has been well documented.[2] Current federal and California laws address only a subset of Smart Grid privacy risks. The numerous Smart Grid components that affect privacy, the division of regulatory authorities and responsibilities between the state and federal levels, and the fact that Smart Grid policies are co-evolving with the grid itself all present challenges to setting privacy rules. Legal protection for Smart Grid data privacy changes as it travels among homes, utilities, and third parties.

Because the Smart Grid is early in its development, however, privacy risks can be efficiently addressed through a combination of sound technology choices and law. If regulators, utilities, and other Smart Grid players take privacy into account when choosing technologies, they will avoid costly retrofits and replacements of equipment and services. In addition, addressing privacy risks now will bolster public trust in this important publicly funded investment in the nation's energy future. Widely used privacy law frameworks, such as Fair Information Practices

---

[1] *See* Smart Grid Interoperability Panel – Cyber Security Working Group, *Guidelines for Smart Grid Cyber Security* 12-54, NISTIR 7628 (July 2010 draft).

[2] *See, e.g.*, *See* Mikhail A. Lisovich, Deirdre K. Mulligan, and Stephen B. Wicker, *Inferring Personal Information from Demand Response Systems*, IEEE SECURITY & PRIVACY, Jan./Feb. 2010, 11-20; Elias Leake Quinn, *Smart Metering & Privacy: Existing Law and Competing Policies* (Spring 2009); Patrick McDaniel & Steven McLaughlin, *Security and Privacy Challenges in the Smart Grid*, IEEE SECURITY & PRIVACY, May/June 2009, 75-77.

and privacy impact assessments,[3] provide ready tools to identify privacy issues in this new technological environment.

Recommendations

Maintaining protections that are reasonably consistent with those that shielded customer privacy in the pre-Smart Grid electricity environment requires immediate action. We recommend the following steps:

- Privacy considerations must drive architectural and information flow design decisions within the network, as well as the policies that cover Smart Grid data held by the growing array of entities who will help reap the benefit of this investment. Because privacy must be embedded in technical design, it cannot be addressed adequately by policies created once technologies are designed and deployed.
- Because privacy risks are fairly consistent across jurisdictions, and the markets for Smart Grid technologies are national, federal policymakers should take the lead in setting legal and technical requirements to protect privacy. NIST, FERC, and the Department of Energy should recognize that the rules, standards, and guidance they develop will determine a great deal about how the Smart Grid develops. They should take advantage of this position to protect privacy.
- State utilities regulators (such as the California Public Utilities Commission) should use their institutional expertise in protecting consumer interests and their broad authority to protect privacy through administrative rules and technical requirements. Both regulatory mechanisms have roles to play in protecting privacy.
- Resolving privacy issues implicates grid cybersecurity, and innovation and competition in the devices and services that operate within the Smart Grid. Regulators at all levels therefore should not consider them in isolation but rather use rulemakings and rate case proceedings to take the interdependencies among these issues fully into account.
- The utilities and technology firms that are building the Smart Grid should protect privacy through their design and implementation of hardware, software, and services.
- Widely accepted information privacy frameworks, such as the Fair Information Practices, combined with privacy-aware design,[4] serve as a useful starting point and should provide the foundation for all Smart Grid players to engage on privacy issues.

---

[3] For a review of Fair Information Practices, see Paul M. Schwartz, *Beyond Lessig's* Code *for Internet Privacy: Cybersapace Control, Filters, and Fair Information Practices*, 2000 WISCONSIN LAW REVIEW 743. For an explanation of privacy impact assessments and how they might be applied to the Smart Grid, see Joint Comments of Center for Democracy & Technology and the Electronic Frontier Foundation on Proposed Findings and Policies Pertaining to the Smart Grid 24-25, 29, CPUC R.08-12-009 (Mar. 9, 2010).

[4] See P. A. Subrahmanyam (Cyberknowledge); David Wagner, Deirdre Mulligan, Erin Jones, Umesh Shankar, and Jack Lerner (University of California at Berkeley), "*Network Security Architecture for Demand Response/Sensor Networks,*" CEC Draft Final Report. Sacramento: California Energy Commission. Oct. 2005, rev. June 2006 (recommending separate data access mechanisms to support systems that do and do not require identifiable data p. 77; and, "when significant computing capability exists inside the home, that processing capability should be developed to enable the customer or his smart equipment to perform

- Regulators conducting federal and state Smart Grid policy proceedings as well as standard-setting bodies should continue to solicit input from privacy experts to ensure that the technical and policy blueprints for the Smart Grid attend to privacy issues.

---

necessary energy-related functions—energy monitoring, demand response control, self-education, and billing—at the home site." P. 78); and, Cavoukian, A., Polonetsky, J., Wolf, C., "*Smart Privacy for the Smart Grid: embedding privacy into the design of electricity conservation,*" Identity in the Information Society, Vol. 3, No. 2 (August 2010), pp. 275-294; and see generally Cavoukian,A., Info. & Privacy Comm'r of Ont., *Privacy by Design*, http://www.privacybydesign.ca/ (last visited November 22, 2010).

CHAPTER 1:
Introduction

1.1 Background

In the century since residential electrical service started to become a ubiquitous feature of life in the United States, the details of how households consume electricity have largely remained inside the home. Electromechanical meters have kept track of total electricity usage, revealing little more than an aggregated figure summarizing how much electricity a household used since the last meter reading. These meters did not record or reveal who used electricity, when, or where, nor did they allow energy consumption to be noted in real-time.

All of this is changing as digital "smart meters" become part of California's (and the nation's) energy infrastructure. Smart meters, as components of the advanced metering infrastructure (AMI), serve a broader effort to construct a "Smart Grid" by integrating information technology into electricity generation, transmission, and distribution. According to the Federal Energy Regulatory Commission (FERC), as of September 2009, there were approximately eight million advanced meters installed nationwide; FERC expects that number to reach 80 to 141 million by 2019.[5] In California, the three major investor-owned utilities (IOUs) are in the midst of deploying smart meters for electricity; they plan to deploy approximately 12 million electric meters by the end of 2012.[6]

Concurrent with this evolution in metering is the development of *home area networks* (HAN) composed of devices that communicate with one another and can communicate data to utilities (or other energy service providers) and can receive and respond to signals sent by these remote entities. An overarching vision of the Smart Grid holds that providing consumers with information about their energy usage will support an array of electricity pricing models and enable customers to better control their electricity use (or authorize a third party to do so).[7]

---

[5] Federal Energy Regulatory Commission, *Assessment of Demand Response and Advanced Metering (Staff Report)* (Sept. 2009), http://www.ferc.gov/legal/staff-reports/sep-09-demand-response.pdf (last visited June 19, 2010).

[6] KEMA, *Final Report for the Meter and Market Assessment Project* 8-20-8-21 (Aug. 2009), http://www.cpuc.ca.gov/NR/rdonlyres/F83E3AA1-7049-4C33-A720-1A3215F4A300/0/CSISolarMeteringReport_Final8409.pdf (last visited June 19, 2010). Pacific Gas & Electric and San Diego Gas & Electric are also deploying smart gas meters. *Id.* at 8-20. This report, however, focuses on electric meters.

[7] *See* Energy Independence and Security Act of 2007 (EISA) § 1306, Pub. L. 110-140 (codified at 42 U.S.C. §§ 17001 *et seq.*); Senate Bill 17 (Padilla, Chapter 327, Statutes of 2009) (codified at CAL. PUB. UTILS. CODE § 8360 *et seq.*). *See also* P.A. Subrahmanyam, David Wagner, Deirdre Mulligan, Erin Jones, Umesh Shankar, and Jack Lerner, *Network Security Architecture for Demand Response/Sensor Networks* 43 (June 2006) (stating that two-way information flows between consumers and utilities or service providers have "the potential to enable a variety of advanced utility applications; such as demand response, energy management services, improved outage management, automation functions, advanced metering and reporting, power quality management, and many other functions") [*CyberKnowledge/Berkeley Report*].

Many details of the architecture(s) that will connect individuals to the Smart Grid, however, remain to be decided.

One end of the design spectrum would rely largely on one-way transmissions of price and event information to customers; energy management systems within customers' homes or businesses would then control networked devices based on these signals and the customer's preferences.

At the other end of the spectrum is a Smart Grid that depends on two-way communications between home devices and utilities or other service providers. In this two-way architecture, a home area network (HAN) gateway[8] enables not only communications between devices inside the home and service providers but also *remote control* of HAN devices . Other architectures are feasible, too. One-way broadcast transmissions of day-ahead price information, for example, have shown promise to achieve significant shifts away from peak demand.

The California Public Utilities Commission has chosen to promote technologies and business models that embrace intensive two-way communications. The CPUC approved utilities' requests to include HAN gateways in their smart meter deployments. The CPUC reasoned that doing so would provide "[t]he most cost effective way . . . over the long term" of realizing the benefits of "enabling price signals, load control and near real time data for residential electric customers."[9] Given the combined size of the major California IOUs' deployments and California's advanced state of Smart Grid activity relative to other states, these decisions are likely to influence other states. Federal policy could provide additional support to this influence. The U.S. Department of Energy, for example, is promoting a bi-directional communications model on the grounds that it will allow individuals and businesses to contribute electricity to the grid and respond to dynamic electricity prices.[10]

But the highly detailed usage and control data that smart meters and HAN gateways transmit also create risks for individual privacy. Instead of providing one data point per month directly to a utility, as was the case with electromechanical meter depicted in Figure 1, the smart meters currently being deployed in California will send hourly readings—hundreds per month—to utilities; and they are capable of taking readings every few seconds for a near-real-time picture of energy consumption.[11]

---

[8] Some sources refer to the HAN gateway as an "electric services interface" (ESI). These two phrases have the same meaning. For consistency, we use HAN gateway throughout this report.

[9] Decision on Pacific Gas and Electric Company's Proposed Upgrade to the SmartMeter Program 176-77, CPUC A.07-12-009 (Mar. 12, 2009).

[10] Dept. of Energy, *Smart Grid System Report* 14-16 (July 2009). The Department of Energy has developed its own Smart Grid privacy analysis. *See* U.S. Department of Energy, Data Access and Privacy Issues Related to Smart Grid Technologies, Oct. 5, 2010, http://www.gc.energy.gov/documents/Broadband_Report_Data_Privacy_10_5.pdf.

[11] *See* Decision Adopting Policies and Findings Pursuant to the Smart Grid Policies Established by the Energy Information [sic] and Security Act of 2007 78, CPUC R.08-12-009 (Dec. 29, 2009) (ordering the three major IOUs in California to "provide to their customers with a smart meter access to usage data on a real-time or near real-time basis no later than the end of 2011"); Southern California Edison's (U-338-E) Reply Comments to Assigned Commissioner and Administrative Law Judge's Joint Ruling Amending

The CPUC currently plans to order the three major IOUs to provide customers and authorized third parties with "near real time" access to energy usage data by the end of 2011.[12] Other states may follow California's example.

This fine-grained data reveals much more than mere electricity consumption: it can reveal when the occupants of a residence are awake or asleep, at home or away.[13] In addition, data from HAN devices can provide distinct data streams that reveal exactly what devices a customer used and when the customer used a given device. Put simply, smart meters currently being deployed offer a direct view into household activities. The clarity of this view will increase as devices connected on home area networks begin to provide more specific usage information and identifiers tied to specific devices.

Figure 1: Pre-Smart Grid Model: Meter data flow from electromechanical meter to utility.

Electromechanical meters measure aggregate electricity consumption at a customer's premises. Utilities read these meters once per month to bill customers for their electricity use. Data flows simply from the home to the utility, the blue building that shows that electricity may come from any of a variety of sources (solar, coal, wind, nuclear, etc.).
Graphics Credit: Brian P. Miller Photo & Design, http://www.brianpmillerphotography.com/

The privacy risks arising from smart meter and HAN device data are legion.[14] Utilities may seek to monetize the information they collect from smart meters.[15] Likewise, third parties may use

---

Scoping Memo and Inviting Comments on Proposed Policies and Findings Pertaining to the Smart Grid 14, CPUC R.08-12-009 (Apr. 7, 2010) ("SCE, PG&E, and SDG&E have plans to provide near real-time usage data, in approximately ten-second increments, to all residential customers."). All documents filed in this CPUC rulemaking ate available at http://docs.cpuc.ca.gov/Published/proceedings/R0812009_doc.htm.

[12] Decision Adopting Policies and Findings Pursuant to the Smart Grid Policies Established by the Energy Information [sic] and Security Act of 2007, D.09-12-046, at 77 (Dec. 17, 2009).

[13] *See* Mikhail A. Lisovich, Deirdre K. Mulligan, and Stephen B. Wicker, *Inferring Personal Information from Demand Response Systems*, IEEE SECURITY & PRIVACY, Jan./Feb. 2010, 11-20; Elias Leake Quinn, *Smart Metering & Privacy: Existing Law and Competing Policies* (Spring 2009).

[14] For a list of risks—including identity theft, real-time surveillance, home invasions, stalking and domestic Abuse–generated by the NIST Privacy Subgroup see Draft slides submitted for use by NIST at Grid Interop November 2009, available at: http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/CSCTGPrivacy (last checked on November 22, 2010).

this data to market products and services.[16] In the wrong hands, this data about electricity usage may indicate when a home is occupied, exposing people and property to potential harm.

Finally, legal privacy protections for utility records were developed around relatively unrevealing data—monthly aggregate consumption, as mentioned above. Going forward, utility records will contain vastly more detailed data generated by interactions with the Smart Grid. The detailed data will make utility records a more attractive investigative tool, thus encouraging access requests by law enforcement agents and litigants in civil lawsuits, such as divorce proceedings. An analogy may be found in the use of cell phone calling records to obtain location information about criminal suspects: the steady increase in the use of cell phones has been accompanied by increasingly dense communications infrastructure that provides increasingly accurate information about a phone's location.[17] These factors have made cell phone location information an increasingly rich tool for law enforcement investigations, though many cell phone users are unaware that their providers have historic data about their location as well as the ability to track them in real-time.[18] Courts and Congress have been slow to adopt or expand rules to regulate law enforcement access to this increasingly sensitive information.[19]

Moreover, Smart Grid data[20] privacy is not an isolated issue. The details of how data flows from meters to customers, utilities, and third parties (and vice versa) also raise several concerns about grid cybersecurity and its openness to innovation, including:

---

[15] Southern California Edison (SCE), *SmartConnect Use Case: C7 – Utility Uses SmartConnect Data for Targeted Marketing Campaigns*, http://www.sce.com/NR/rdonlyres/E2927535-15B3-41F3-AE88-B06CE760225F/0/C7_Use_Case_081229.pdf

[16] Southern California Edison (SCE), *SmartConnect Use Case: C7 – Utility Uses SmartConnect Data for Targeted Marketing Campaigns*, http://www.sce.com/NR/rdonlyres/E2927535-15B3-41F3-AE88-B06CE760225F/0/C7_Use_Case_081229.pdf.

[17] The rapid growth in the popularity of cell phones, the continuing deployment of cell phone infrastructure, and advances in phone-based geolocation technologies (e.g., GPS), have made location information possessed by cell phone service providers an increasingly used—and useful—tool for law enforcement investigations. *See In re* Application of the United States of America for an Order Directing a Provider of Electronic Communications Service to Disclose Records to the Government, No. 07-524M, slip. op. at 8-10 (W.D. Pa., Feb. 19, 2008) (noting ten-fold growth in number of U.S. cell phone users from 1994 to 2006 and ability of cell service providers to localize a phone to a 200-foot radius in some areas).

[18] *Id.* at 3 (stating that cell site location information is "broadly sought" by law enforcement agencies).

[19] *See id.* at 10-23 (reviewing relevant laws). Still, the law *does* evolve. For example, the U.S. Court of Appeals for the D.C. Circuit recently held that police tracking of all of a suspect's movements over the course of a month via GPS was a search subject to the Fourth Amendment's reasonableness requirements. United States v. Maynard, No. 08-3030, slip op. at 16-34 (D.C. Cir., Aug. 3, 2010). The court noted that, while many movements are exposed to the public, "prolonged GPS monitoring reveals an intimate picture of the subject's life that he expects no one to have—short perhaps of his spouse." *Id.* at 32. *But see also* United States v. Pineda-Moreno, No. 08-30385 (9th Cir., Jan. 11, 2010) (holding that police use of a mobile tracking device on a suspect's car was not a search at all).

[20] We use "Smart Grid data" as an umbrella terms that refers to information pertaining to residential customers' electricity usage. As discussed in more detail in Chapter 3, this data includes consumption data, price information, and HAN device control traffic.

- **Unauthorized access to personal data.** Keeping data secure against misuse and disclosure through malicious attacks, accidental leaks, and insider abuse is critical to protecting customers' privacy interests. This requires a combination of technical mechanisms—in meters, the data transmission pathway, and the systems of utilities and other Smart Grid data recipients—and sound data governance practices.

- **Registration of smart devices on home area networks.** Establishing secure communications channels between a home area network gateway (HAN gateway) and a device on the home area network (HAN device) is important for privacy and other reasons. One way of accomplishing this is by limiting communication to those devices registered with the entity that controls the HAN gateway.[21] One obvious choice to control the HAN gateway is the customer, which would be analogous to how individuals control their home wireless networks. By allowing consumers to connect any device that can communicate using a widely adopted and open network protocol, wireless routers have supported the development and introduction of countless varieties of devices and services. Alternatively, utilities could be given control over the HAN gateway—which currently appears to be a likely outcome in several jurisdictions—allowing utilities to decide which devices a consumer can connect to the HAN gateway. In this scenario, the utility's decisions about which devices to permit or deny could be unfettered. It remains unclear what criteria utilities will use to accept or reject—or whether regulations or guidance will be issued on this point—a customer's device registration request. In this model, utilities become gatekeepers of the home area network and are in the position to thwart consumer choice and competition in the emerging market for smart devices, including competition around privacy and security features.

- **Access by non-utility third parties to smart meters.** Allowing third parties to obtain near-real-time electricity usage data could allow energy management services to compete along dimensions of price, quality, and privacy without requiring customers to purchase their own measurement devices. Establishing such third-party access will require balancing security requirements (such as the need to authenticate a party who wishes to access a meter) with a process that sets clear, non-discriminatory conditions for third-party access. It also requires privacy rules that flow with consumers' Smart Grid data.

- **Visibility into home area networks.** Device registration or other aspects of communicating with devices on home area networks will likely expose device-specific data streams to utilities or third parties. These data streams will make it relatively simple for utilities or third parties to develop detailed customer profiles, including what kinds of devices a customer uses and when. With less precision, utilities and third parties may also be able to infer *where* a customer was active in the home by analyzing device-specific data streams or combining fine-grained energy usage information with auxiliary information about a home, such as its floor plan and the appliances inside.

---

[21] UCAIug OpenHAN Task Force, *UCAIug Home Area Network System Requirements Specification v1.95* at 30, "The Registration process is a further step involving Mutual Authentication and authorizing a Commissioned HAN device to exchange secure information with other Registered devices and with an ESI."

We highlight the intersection of privacy, security, and innovation issues throughout the report.

1.2 Project Approach

Our analysis of privacy in the Smart Grid considers the technologies and standards most relevant to AMI deployment in California. We gathered information about the current and future capabilities of the smart meters being deployed by the three major California investor-owned utilities (IOUs). This was supplemented with the standards, guidelines, and use cases driving the NIST process—the key federal activity generating smart grid deployment technology and policy—to develop a holistic picture of what data of residential customers will go where, and what the recipient(s) plan to do with it. The key documents in this analysis are:[22]

- NIST's *Framework and Roadmap of Smart Grid Interoperability Standards*;
- The NIST Smart Grid Interoperability Panel Cyber Security Working Group's *Guidelines for Smart Grid Cyber Security*, which includes an extensive analysis of privacy issues;[23]
- Southern California Edison's AMI and Smart Grid use cases;
- ZigBee Alliance and HomePlug Powerline Alliance Smart Energy Profile 2.0 documents;
- The UCA International Users Group (UCAIug) OpenHAN Task Force's *Home Area Network System Requirements Specification;*[24]
- Decisions, orders, rulings, and comments, and other documents filed in the California Public Utilities Commission's Smart Grid policy rulemaking[25] and advanced metering infrastructure proceedings.[26]

Through this review, we identified a set of key actors (e.g., customers, utilities, third parties, regulators) and technologies (e.g., smart meters, home area network gateways) that constitute the Smart Grid and developed a set of information flows that capture their interactions. Based on these information flows, we conducted a privacy analysis informed by the legal authorities (statutes and regulations, federal and state constitutional rights, and enforcement agencies) that may play a role in protecting privacy interests in Smart Grid data. For each information flow, we identify both the sources of, and the gaps in, privacy protection. This analysis provides a picture of how current privacy rules—which reflect the high degree of protection afforded to in-home activities as well as the assumption that electricity metering technologies would not

---

[22] Many of these documents were drafts (and some remain drafts) or form an expanding corpus of documents. We have tried to refer to the most recent documents, but it is inevitable that some of these documents will be superseded.

[23] http://collaborate.nist.gov/twiki-sggrid/pub/SmartGrid/NISTIR7628v1July2010/draft-nistir-7628_whole_07-06-10.doc.

[24] Draft 1.95 (May 21, 2010) of Version 2.0, *available at* http://osgug.ucaiug.org/sgsystems/openhan/Shared%20Documents/OpenHAN%202.0/UCAIug%20OpenHAN%20SRS%20-%20v1.95%20clean.doc.

[25] *See* CPUC, All Documents for Proceeding R0812009, http://docs.cpuc.ca.gov/Published/proceedings/R0812009_doc.htm (last visited June 7, 2010).

[26] See Appendix A for a list of relevant CPUC documents.

expose those activities to the outside world—will carry forward in a radically altered technological environment.[27]

1.3 Scope and Organization of this Report

Smart Grid privacy concerns are most acute for residential utility customers. Thus, our report focuses on the *distribution* portion of the electric grid, as well as electricity storage and generation technologies that residential customers are likely to adopt on a large scale (e.g., plug-in electric vehicles). When technologies and policies differ for residential versus commercial and industrial customers, we examine only the residential questions in detail. Unless otherwise noted, we use the term **customer** to refer to an individual who has a privacy interest in data about energy use at a residence.

In addition, we focus on developments in California. Though federal law and policy features prominently in this report, state-level regulation is central to understanding Smart Grid privacy. California is an appropriate case study for two reasons: the state's major investor-owned utilities are moving quickly to install residential smart meters on a large scale (i.e., millions of meters), and the California Public Utilities Commission's Smart Grid policy rulemaking illustrates the potential breadth of utility regulators' authority to address privacy issues.

Given that the legal protections for Smart Grid data depend heavily upon the details of how the data flows, we have organized our report around different stages and patterns of information flow. Chapter 2 provides a brief overview of the federal and California policies that have set the stage for Smart Grid deployment, as well as a brief introduction to the key Smart Grid components. Chapter 3 focuses on different scenarios for electricity usage data flow through these components. Specifically, it discusses eight information flow patterns in detail, highlighting the types of devices and entities that handle data in each case. A discussion of the privacy and related security and innovation issues follows each description.

[27] One of us has argued that policymakers should establish privacy rules for customer usage data. *See* Jack Lerner & Deirdre K. Mulligan, *Taking the Long View on the Fourth Amendment: Stored Records and the Sanctity of the Home*, 2008 STAN. TECH. L. REV. 3. But advancing those policy preferences is not the aim of this report.

CHAPTER 2:
Policy Frameworks: Smart Grid and Information Privacy

2.1 Federal Smart Grid Policy

A national vision for the Smart Grid, articulated in the Energy Independence and Security Act of 2007 (EISA), highlights the potential for information about prices, supply and demand, and outages to help reduce peak demand, incorporate renewable energy sources and distributed generation, and speed recovery from interruptions.[28] These changes in how the grid operates, in turn, have the potential to reduce the projected growth in energy demand, prices, and carbon emissions.[29]

The foundation of this plan is to integrate information technology into the electric grid. The National Institute of Standards and Technology (NIST) is coordinating an effort to foster interoperability, security, and privacy. EISA also directs the Federal Energy Regulatory Commission (FERC) to adopt Smart Grid standards and protocols through a rulemaking, once NIST's efforts have "led to sufficient consensus."[30] According to its Smart Grid policy statement, FERC understands its mandate under EISA to include setting standards that "will be applicable" to "all elements of the grid, including communications with the ultimate consumer."[31] FERC, however, is unlikely to *require* states or utilities to adopt or use these standards.[32] To lay the groundwork for this rulemaking, FERC released a Smart Grid Policy Statement, which sets forth FERC policy on cybersecurity, electric vehicles, and variable electricity generation as they relate to the bulk-power system. The Department of Energy (DOE) has an ongoing role in assessing Smart Grid deployments and technology under EISA.[33]

---

[28] Pub. L. 110-140 §§ 1301, 1306.

[29] *See* U.S. Department of Energy, *What the Smart Grid Means to You and the People You Represent* 2-3 (in *Smart Grid Stakeholders Books* series) (2009), http://www.oe.energy.gov/DocumentsandMedia/Regulators.pdf (stating that "[e]lectricity prices are forecast to increase 50% over the next 7 years"; "[n]ationwide, demand for electricity is expected to grow by 30% by 2030"; and "[i]f we do nothing, U.S. carbon emissions are expected to rise from 1700 million tons of carbon per year today to 2300 million tons of carbon by the year 2030") (citations omitted).

[30] EISA § 1305(d) (directing FERC to adopt standards and protocols to "insure smart-grid functionality and interoperability in interstate transmission of electric power, and regional and wholesale electricity markets").

[31] FERC, Smart Grid Policy, 74 Fed. Reg. 37,098-01 ¶ 22 (July 27, 2009).

[32] *See* FERC, Smart Grid Policy, 74 Fed. Reg. 37,098-01 ¶ 23 (July 27, 2009) ("EISA, however, does not make any standards mandatory and does not give the Commission authority to make or enforce any such standards. Under current law, the Commission's authority, if any, to make smart grid standards mandatory must derive from the FPA.").

[33] EISA § 1302 (requiring DOE to report regularly to Congress on "the status of smart grid deployments nationwide and any regulatory or government barriers to continued deployment").

The American Recovery and Reinvestment Act of 2009 (ARRA)[34] accelerated NIST's work in particular[35] and Smart Grid deployment in general. Under the ARRA, Congress appropriated more than four billion dollars to fund Smart Grid demonstration and pilot projects, which range from deploying smart meters to examining new types of energy storage systems. DOE helped select projects for ARRA funding.[36]

Several federal agencies have taken an interest in Smart Grid privacy issues, but none has issued binding privacy regulations. NIST, through its Cyber Security Working Group, has developed an extensive analysis of privacy risks,[37] as well as a framework for Smart Grid actors and customers to use to assess privacy risks.[38] The White House Office of Science and Technology Policy issued two requests for public comments on consumer-related Smart Grid issues, including privacy.[39] Finally, DOE issued its own request for information concerning data access and privacy issues.[40]

2.2 California Smart Grid Policy

The federal efforts discussed above provide some coordination for state-level and commercial activities surrounding the Smart Grid. Nonetheless, many Smart Grid technology and policy decisions will be made on a state-by-state level.

For example, the State of California has developed its own Smart Grid-related policies over the last decade. This development began in the wake of the 2000-2001 energy crisis, when the California Energy Commission and the California Public Utilities Commission (CPUC)

---

[34] Pub. L. 111-5 (2009).

[35] The Energy Independence and Security Act (EISA) of 2007, tasked the National Institute of Standards and Technology (NIST) with the "primary responsibility to coordinate development of a framework that includes protocols and model standards for information management to achieve interoperability of smart grid devices and systems..." The American Recovery and Reinvestment Act (ARRA), provided NIST with $10 million to carry out these tasks. For an overview of NIST's work see the NIST Smart rid Interoperability Standards Project http://www.nist.gov/smartgrid/ (last visited November 22, 2010), and the NIST Smart Grid Collaboration Site http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/WebHome (last visited November 22, 2010).

[36] *See* U.S. Dept. of Energy, American Recover and Reinvestment Act, http://www.oe.energy.gov/american_recovery_reinvestment_act.htm (last visited July 14, 2010) (linking to resources that detail ARRA spending on Smart Grid projects).

[37] NIST Interagency Report (NISTIR) 7628, *Guidelines for Smart Grid Security, Vol. 2: Privacy and the Smart Grid*, §§ 5.6, Aug. 2010, http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol2.pdf.

[38] *Id.* § 5.4 (explaining consumer-to-utility privacy impact analysis methodology).

[39] Office of Science and Technology Policy, Notice and Request for Comment on Consumer Interface With the Smart Grid, 75 Fed. Reg. 7526 (Feb. 19, 2010); Office of Science and Technology Policy, Notice and Request for Public Comment on the Consumer Interface with the Smart Grid, 75 Fed. Reg. 6414 (Feb. 9, 2010), http://edocket.access.gpo.gov/2010/2010-2813.htm.

[40] U.S. Dept. of Energy, Request for Information, 75 Fed. Reg. 26,203 (May 11, 2010).

instituted demand response programs to reduce peak energy demand.[41] The Legislature mandated a study of dynamic pricing for residential and commercial customers.[42]

In a related rulemaking, the CPUC and the Energy Commission developed six functional criteria for the state's AMI.[43] These requirements include: the capability to collect usage data at hourly intervals for residential customers; a means of providing customers with flexible access to data about their energy usage; and the capability to interface with "load control communication technology."[44]

Subsequently, Pacific Gas & Electric (PG&E), Southern California Edison (SCE), and San Diego Gas & Electric (SDG&E) submitted their AMI business cases, which the CPUC approved between 2006 and 2009.[45] PG&E, SCE, SDG&E are currently actively engaged in AMI deployment, which is expected to take until 2011 or 2012 to complete.[46]

Consistent with the CPUC's AMI functional criteria, IOUs' smart meters collect hourly data on residential energy usage and provide day-after access via the utilities' websites. The CPUC has also approved plans for all three major California IOUs to embed HAN gateways in their smart meters. Appendix A provides a summary of the AMI architectures under deployment in California.

Energy usage information privacy is a significant element of a CPUC rulemaking[47] undertaken as part of the CPUC's development of a comprehensive Smart Grid policy in response to state[48]

---

[41] *See* Order Instituting Rulemaking, CPUC R.02-06-001. Documents filed in this rulemaking are available at http://docs.cpuc.ca.gov/published/proceedings/R0206001_doc.htm (last visited May 13, 2010).

[42] Reports from the pricing pilot study are available at http://energyarchive.ca.gov/demandresponse/documents/index.html (last visited May 13, 2010).

[43] Joint Assigned Commissioner and Administrative Law Judge's Ruling Providing Guidance for the Advanced Metering Infrastructure Business Case Analysis 3-4, CPUC R.02-06-001, Feb. 19, 2004.

[44] *Id.*

[45] See Appendix A for a list of relevant CPUC documents.

[46] KEMA, *Final Report for the Meter and Market Assessment Project* 8-20-8-21 (Aug. 2009), http://www.cpuc.ca.gov/NR/rdonlyres/F83E3AA1-7049-4C33-A720-1A3215F4A300/0/CSISolarMeteringReport_Final8409.pdf (last visited June 19, 2010).

[47] The CPUC recently declined to adopt a privacy rule and will instead continue to develop the record on privacy issues in its Smart Grid rulemaking. *See* Decision Adopting Requirements for Smart Grid Deployment Plans Pursuant to Senate Bill 17 (Padilla), Chapter 327, Statutes of 2009, at 121, CPUC R.08-12-009, June 28, 2010 ("[W]e will embark on a phase of this proceeding to develop security and privacy procedures in more detail, and we will not order third-party access to information until such measures are in place.").

[48] SB 17, which was signed by Governor Arnold Schwarzenegger on October 11, 2009, articulates high-level goals for the Smart Grid in California, including increasing energy efficiency, incorporating renewable energy sources and distributed generation, and promoting the deployment and integration of smart technologies. CAL. PUB. UTILS. CODE § 8360. SB 17 also directs the CPUC to set requirements for utility Smart Grid deployment plans to reflect these priorities by July 1, 2010.

and federal legislation.[49] The need for a privacy rule that applies to third parties as well as utilities has been a subject of extensive commentary. All signs—technical standards, state and federal policy, and developments in the marketplace—point toward an important role for third-party collection and analysis of energy usage information. As several parties have pointed out, third-party storage also creates significant privacy risks by making it relatively easy for law enforcement agencies, civil litigants, and commercial entities to obtain energy usage information. Exactly what restrictions those parties face in obtaining data depends heavily upon the characteristics of the data, who controls it, and who seeks it. Chapter 3 of this report examines those restrictions in detail.

Currently, SDG&E is the only major California IOU that allows customers to request transfer of their energy usage information to a third-party partner.[50] There is broad agreement among parties that existing regulations provide few specific constraints on how third parties may collect, use, and disclose energy usage information; and, in contrast to utilities, third parties are not closely overseen by a regulator such as the CPUC. The CPUC will issue a privacy rule later in the rulemaking; at this point it is unclear whether the rule will regulate all third parties that handle energy usage information.[51] It is also unclear whether the final rule will place the same obligations on third parties as on investor-owned utilities.[52]

---

[49] The Energy Independence and Security Act of 2007 (EISA) § 1307 directs state utilities regulators to "consider requiring that, prior to undertaking investments in nonadvanced grid technologies, an electric utility of the State demonstrate to the State that the electric utility considered investment in a qualified smart grid system based on appropriate factors . . ." (codified at 16 U.S.C. § 2621). The CPUC's gloss on this directive is that it "impose[s] on states an obligation to determine whether to adopt a specific statutory standard as consistent with the purposes of the act and then to determine whether to impose the standard on each utility subject to state ratemaking jurisdiction. The law delegates to the state broad power, to the extent consistent with state law, to determine the specific requirements of the standards." Decision Adopting Policies and Findings Pursuant to the Smart Grid Policies Established by the Energy Information [sic] and Security Act of 2007, at 15, CPUC R.08-12-009, Dec. 17, 2009. The Commission determined that its December 2009 ruling, *id.*, met EISA's obligations; but the rulemaking continues in order to fulfill the requirements of SB 17 as well as set Smart Grid policies that are consistent with existing state renewable energy, distributed generation, and demand response policies. Assigned Commissioner and Administrative Law Judge's Joint Ruling Amending Scoping Memo and Inviting Comments on Proposed Policies and Findings Pertaining to the Smart Grid, at 3-4, CPUC R.08-12-009, Feb. 8, 2010.

[50] SDG&E partnered with Google, allowing SDG&E customers to enroll in Google's PowerMeter service. *See* SDG&E, Monitor Your Home Electricity Use with Google PowerMeter, http://www.sdge.com/myaccount/energynetwork/ (last visited Oct. 26, 2010).

The CPUC has expressed its intention of ordering third-party access by the end of 2010. Decision Adopting Policies and Findings Pursuant to the Smart Grid Policies Established by the Energy Information [sic] and Security Act of 2007, D.09-12-046, at 65, CPUC R.08-12-009, Dec. 17, 2009. ("We will require that by the end of 2010, the utilities will have put into place operations that allow customers to access their information easily through an agreement with a third party, provided sufficient privacy and security measures are in place to mitigate the potential for fraud and hacking."); *id.* at 78 (formally ordering the same). But the CPUC also recently ruled that it will not order third-party access until it has adopted access rules. *See supra* note 30.

[51] Several small investor-owned utilities (IOUs) in California were dismissed from the CPUC's Smart Grid policy rulemaking because the "small size of these utilities and the nature of their operations both

2.3 Relating Smart Grid Architecture to Information Privacy Frameworks

Before we delve into the details of Smart Grid information flows and their attending privacy risks, it is useful to consider key architectural choices that inform data flow in the Smart Grid and therefore substantively influence the possible privacy outcomes. As the discussion in Chapter 3 will make evident, privacy risks depend heavily upon the characteristics of a given data flow—the nature of the data, who receives data, and what a given entity plans to do with data.

Attending to privacy issues is considerably simpler if a semi-permeable boundary is drawn around customers' homes, say at the electric meter, that lets information in but not out. This would be a high-level privacy aware design strategy. Conceptually speaking, utilities and device manufacturers could be made subject to a principle of minimizing HAN devices' dependence on communicating with entities outside the home. A high-level architecture that might emerge from this approach is one in which utilities broadcast one-way price and event signals. Customers' energy management systems would control HAN devices based on these signals and customers' preferences, such as whether they will tolerate electricity interruptions for certain devices. The smart meter would serve only the basic function of reporting to the utility how much electricity a customer consumed, and when.

Though setting up a one-way gate for information around the home would mitigate many of the privacy risks we discuss in Chapter 3,[53] this approach is also at odds with policies in California and elsewhere encouraging the development of two-way communications involving smart meters and HAN gateways. Moreover, Smart Grid policy in California, in other states, and at the national level envisions expansive roles for third parties. Absent a reversal of these policies, the complicated privacy and security risks involving information flows in and out of the home, increasing access by third parties, and remote management of in-home devices must be addressed with a more nuanced and integrated approach.

If, as current trends indicate, California and the nation choose to embed two-way communication within the Smart Grid, developing a conceptual map of important data flows and a privacy framework to guide technical and policy choices becomes ever more essential.

Appropriately, Smart Grid policy makers—the CPUC and NIST, in particular—and participants in the proceedings[54] have embraced frameworks based on a set of "Fair Information Practice"

---

increase the costs and diminish the benefits of the EISA requirements." Decisions Adopting Policies and Findings Pursuant to the Smart Grid Policies Established by the Energy Information and Security [sic] Act of 2007, at 2, CPUC R.08-12-009, Dec. 17, 2009. This left the three major IOUs—Pacific Gas & Electric, Southern California Edison, and San Diego Gas & Electric—as parties. Publicly owned utilities are not subject to CPUC jurisdiction.

[52] See section 3.1.2.

[53] Meter data collected at short time intervals would not be eliminated under this approach. This type of Smart Grid data carries its own privacy risks.

[54] *See* Joint Comments of Center for Democracy & Technology and the Electronic Frontier Foundation on Proposed Findings and Policies Pertaining to the Smart Grid 14-26 (filed with CPUC, Mar. 9, 2010).

principles (FIPs) that establish ongoing rights and obligations to govern information about individuals held by smart grid players.[55] FIPs conceptualize privacy as the right to informational self-determination that affords individuals control over personal information to protect individual autonomy, self-development, and intimacy.[56] Statements of the FIPs vary, but a recent statement by the Department of Homeland Security provides widely accepted principles and definitions.[57] In DHS's statement, FIPs comprise the following principles:

- **Transparency:** organizations should provide notice to individuals regarding their use, disclosure, and retention of personally identifiable information (PII).
- **Individual participation:** organizations should seek individual consent to collect, disclose, and retain PII.
- **Purpose specification:** organizations should articulate specific purposes for collecting PII, and specific uses for PII they collect.
- **Data minimization:** organizations should collect only PII that is "directly relevant and necessary to accomplish the specified purpose(s)" and retain data no longer than necessary.
- **Use limitation:** organizations should use PII only for the purposes stated in their notices.

---

[55] Another way to view Smart Grid privacy would be in terms of information ownership; that is, ask simply, "Who owns the data?" This property-based framework was popularized in Lawrence Lessig's *Code and Other Laws of Cyberspace* (1999) (see in particular pp. 156-163) but has few followers among privacy law scholars and practitioners. *See* Marc Rotenberg, *Fair Information Practices and the Architecture of Privacy (What Larry Doesn't Get)*, 2001 STANFORD TECHNOLOGY LAW REVIEW 1, http://stlr.stanford.edu/STLR/Articles/01_STLR_1; Paul M. Schwartz, *Beyond Lessig's* Code *for Internet Privacy: Cyberspace Filters, Privacy-Control, and Fair Information Practices*, 2000 WISCONSIN LAW REVIEW 743. It is inaccurate to describe U.S. privacy statutes as taking a property-based approach. Numerous information privacy statutes—including the Video Privacy Protection Act, the Privacy Act, and the Cable Communications Act, among others—provide detailed rules to protect individuals' expectations of privacy in transactions involving transfers of data for specifically stated purposes. *See* Schwartz, *Beyond Lessig's* Code, at 779; Rotenberg, *Fair Information Practices*, ¶¶ 26-35.

Unfortunately, viewing personal information as property has gained a following among policymakers. *See, e.g.*, Office of Science and Technology Policy, Notice and Request for Public Comment, 75 Fed. Reg. 7526, 7527 (seeking comment on the question, "Who owns the home energy usage data?"). *See also* Department of Energy, Request for Information: Implementing the National Broadband Plan by Empowering Consumers and he Smart Grid: Data Access, Third Party Use, and Privacy, 75 Fed. Reg. 26,203 (May 11, 2010) (seeking comment on "[w]ho owns energy consumption data").

[56] This conception of privacy goes back to some of the earliest legal scholarship on privacy law. *See* Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, HARVARD LAW REVIEW, vol. 4, p. 193 (1891). For a recent review of the state of privacy law and scholarship, see Daniel J. Solove, *A Taxonomy of Privacy*, 154 UNIVERSITY OF PENNSYLVANIA LAW REVIEW 477 (2006).

[57] Issued Dec. 28, 2008, *at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf.

- **Data quality and integrity:** organizations should keep PII accurate, relevant, timely, and complete.
- **Security:** organizations should implement adequate safeguards to protect against loss, unauthorized use, modification, and unintended disclosure.
- **Accountability and auditing:** organizations should audit employees' and contractors' actual use of PII, to ensure compliance with the other FIPs.

While few U.S. information privacy statutes implement all of these principles, and U.S. privacy laws are typically limited to specific types of information (e.g., telecommunications records; healthcare information) and relationships (e.g., the customer-service provider relationship in the telecommunications sector; or patient-physician), FIPs are broadly accepted world-wide as the operational reference for privacy rights and obligations. For this reason, the constituent principles provide a useful guide throughout the remainder of this report.

CHAPTER 3:
Privacy Risks in Smart Grid Information Flows

Smart Grid data will not follow a single, well-defined pathway. Instead, the Smart Grid will support a variety of information flows. This chapter provides a detailed look at those information flows, both at the technical level (which devices are involved and which actors have access to information) and at the legal level (which statutes and regulations currently apply).

This report adopts terms that reflect the separation of the meter and the HAN gateway, as well as the distinction between data about energy consumption and information that can be used to manage or control devices.

Meter data: any data collected by a utility-owned electric meter.[1]

Energy usage information: consumption and time-of-use, which can be measured by a range of devices, including customer-owned metering devices that send data directly to third parties.[1]

Load control information: information that helps achieve demand response, particularly through automated means.[1] Prices and device control signals are examples. Load management information

3.1 Meter Data and Energy Usage Information Privacy Risks

3.1.1 Meter Data Sent from Meter to Utility

A fundamental data flow in the Smart Grid involves meter data going from the meter to the utility.[58] The utility-provided meter measures electricity consumption over time and may store it before transmitting the data to the utility. Smart meters are capable of taking readings every few seconds, but in California at least, they do not send such fine-grained data to utilities. Instead, smart meters send hourly data to utilities, typically in several batches per day.[59]

[58] The terms used in the report are drawn from several sources: SmartGrid/AEIC AMI Interoperability Standard Guidelines for ANSI C12.19 End Device Communications and Supporting Enterprise Devices, Networks and Related Accessories Version 2.0, Draft 8, Revision 3, at 11-20 (June 10, 2010), http://collaborate.nist.gov/twiki-sggrid/pub/SmartGrid/PAP05MeterProfiles/SmartGrid-AEIC-Standard-For-Interoperability-v2.0-DRAFT-8.3--06-10-10.doc; Smart Grid Interoperability Panel, PAP10: Standard Energy Usage Information, http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/PAP10EnergyUsagetoEMS (last visited Aug. 26, 2010) (describing PAP10's purpose as the development of "data standards to exchange fine grained and timely information about energy usage"); and California Energy Commission, Proposed Load Management Standards (Draft Committee Report), at 1-2, CEC-400-2008-027-CTD (Nov. 2008), http://www.energy.ca.gov/2008publications/CEC-400-2008-027/CEC-400-2008-027-CTD.PDF.

[59] Based on informal discussions with CPUC staff and individuals knowledgeable about current smart meter technology, we understand that the smart meters deployed by California IOUs transmit customer usage data three times per day. This scheduling is necessary to avoid creating congestion in the utilities' backhaul networks. Thus, while the utilities collect, and provide to customers or third parties, data at hourly increments, there may be a lag of several hours between measurement by the meter and transmission to the utility. Moreover, usage data generally is not available to customers until the next day. *See supra* notes 34 and 36.

Utilities use meter data for a variety of purposes. They use fine-grained meter data to apply time-variant pricing, including time-of-use rates, critical peak pricing, and real-time pricing.[60] Utilities may also use meter data for load research, e.g., to better understand which devices customers are using at a given time.[61] Data mining algorithms may help utilities sell targeted advertising to customers.[62] A utility might detect meter tampering by comparing current data with historical records.[63] Utilities also make the data available to customers through their websites to improve customers' understanding of their energy usage and promote load shifting to reduce peak demand.[64]

This information flow raises several privacy issues. The discussion below illustrates how legal protections vary depending on where and how the data is accessed.

Figure 2: Meter data flow between smart meter and utility

A smart meter (in magenta, attached to the side of the house) collects, stores, and transmits short-interval meter data from the home to the utility (drawn in blue). Smart meters also facilitate two-way communications between the meter and the utility. Energy usage information is depicted as a bidirectional arrow composed of discrete square elements.
Graphics Credit: Brian P. Miller Photo & Design, http://www.brianpmillerphotography/

[60] CAL. PUB. UTILS. CODE § 502(c) ("The commission may, at any time, authorize an electrical corporation to offer residential customers the option of receiving service pursuant to time-variant pricing and to participate in other demand response programs."); CAL. PUB. UTILS. CODE § 502(a)(2) ("'Time-variant pricing' includes time-of-use rates, critical peak pricing, and real-time pricing, but does not include programs that provide customers with discounts from standard tariff rates as an incentive to reduce consumption at certain times, including peak time rebates."); CAL. PUB. UTILS. CODE § 745 (forbidding utilities from "employ[ing] mandatory or default time-variant pricing" before January 1, 2013).

[61] SCE, *SmartConnect Use Case: C8 – Load Researchers Perform Analyses Using SmartConnect Data*, http://www.sce.com/NR/rdonlyres/D7F9B623-2DA0-4E31-A98C-5537748279BB/0/C8_Use_Case_090120.pdf (last visited June 19, 2010).

[62] SCE, *SmartConnect Use Case: C7 – Utility Uses SmartConnect Data for Targeted Marketing Campaigns*, http://www.sce.com/NR/rdonlyres/E2927535-15B3-41F3-AE88-B06CE760225F/0/C7_Use_Case_081229.pdf (last visited June 19, 2010).

[63] SCE, *SmartConnect Use Case: B3 - Utility detects tampering or theft at customer site*, http://www.sce.com/NR/rdonlyres/943C8D62-0011-4959-9C5A-620684B34CF3/0/ARCHB3USECASEv12050106.pdf (last visited June 19, 2010).

[64] *See* Cal. Pub. Utils. Code § 8360(d) (specifying demand response as a grid modernization policy goal); *id.* § 8366(d) (same).

3.1.1.1 Data stored in meter

Smart meters store meter data internally. Under current AMI architectures, utilities control the meters; they do not grant access to other parties without customer's consent. But suppose that some individual—a hacker or a burglar, for example—wants to obtain data about a specific customer and takes advantage of the smart meter's network connection to remotely hack into the meter. Unlike a mechanical meter, which requires proximity to access and provides no historical data about energy usage, smart meters can be broken into remotely and contain an uncertain amount of data about occupant behavior. This information could facilitate threats to a customer's physical security by providing detailed information about when he or she is at home.

Since smart meters apply access controls to stored data (and hence provide a technology-based means for authorizing access to data), this conduct is prohibited under state and federal "anti-hacking" laws. Specifically, the federal Computer Fraud and Abuse Act (CFAA) prohibits accessing a "protected computer" without authorization or in excess of authorization. To the extent that smart meters and other smart grid components are "computers" within the meaning of the CFAA,[65] the statute prohibits others from breaking into them and thereby obtaining information. At the state level, California prohibits obtaining data by knowingly gaining unauthorized access to a computer,[66] such as a smart meter. A qualification to applying these laws to smart meter intrusions is that an intrusion must cause "loss" to constitute an offense. Loss is defined broadly under the CFAA to include "any reasonable cost to any victim," including the costs of responding to an intrusion, restoring lost data, and lost revenue resulting from an incident.[67]

Two characteristics of computer abuse statutes distinguish them from many of the other laws and regulations discussed in this report. First, they apply to "information" and "data." These broad terms presuppose nothing about the value of the data to the customer, the utility, or any other party. Nor do they require that the information be "personally identifiable" or "private."

Second, neither federal nor state computer abuse laws require the owner of a computer system to provide any particular level of technical protection for data in order to qualify for relief. In principle, data stored on a smart meter, and protected only by a widely known, globally used password could still be protected from unauthorized access under federal and state laws. Note that, although the utility owns the meter, the CFAA permits "[a]ny person who suffers damage or loss by reason of a violation" of the Act to sue for damages."[68] Thus, if a customer suffers sufficient loss as a result of a hacked meter, he or she may file a civil suit against the

---

[65] A computer is "protected" by the CFAA if it is used in or affects interstate or foreign commerce. 18 U.S.C. § 1030(e). This definition is jurisdictional; "protected" here simply means that a computer is covered by the CFAA, not that it is protected against unauthorized access in any technical, or even contractual, sense.

[66] Cal. Penal Code § 502. All 50 states have similar laws. *See* Susan W. Brenner, *State Cybercrime Legislation in the United States of America: A Survey*, 7 RICH. J.L. & TECH. 28, ¶ 15 n.37 (2001), *at* www.richmond.edu/jolt/v7i3/article2.html (listing the laws).

[67] 18 U.S.C. § 1030(e)(11).

[68] 18 U.S.C. § 1030(g); *see also* Expert Janitorial, LLC v. Williams, 2010 WL 908740 (E.D. Tenn., Mar. 12, 2010).

perpetrator.[69] In addition, the utility may sue civilly if it suffers loss (e.g., by conducting a forensic investigation of the incident, sending a technician to replace the meter, etc.). Finally, the government may file criminal charges against the party (or parties) who gain unauthorized access to a smart meter.

3.1.1.2 Data in transit.

As data moves from the smart meter to the utility—typically via a radio frequency network that the utility operates solely for its own use—a separate set of statutes protects data confidentiality. The federal Wiretap Act prohibits a person who is not a party to a communication from intentionally "intercepting" the communication.[70] The California Penal Code contains a similar prohibition.[71] As with computer fraud laws, anti-wiretapping laws do not require the parties to the communication—the utility and the customer in this case—to take technical precautions (e.g., encrypting the contents of the communication) against interception. There is an exemption to the Wiretap Act for "an electronic communication made through an electronic communication system that is configured so that such electronic communication is readily accessible to the general public."[72] If utilities used radio-frequency broadcasts to transmit price information, for example, those communications would probably be exempt from the Wiretap Act. Communications between a smart meter and a utility over a cellular or spread-spectrum network, however, involve well-defined senders and recipients and, at a technical level are not "readily accessible to the general public." As a result, they would be protected by the Wiretap Act.

3.1.1.3 Data retained by utility.

Once meter data reaches the utility, a customer's privacy interests are legally protected in two distinct ways. First, like data stored on a smart meter, meter data stored on a utility's computers is protected by federal and state anti-hacking laws.

Second, once a utility acquires data from a customer's smart meter, it has certain affirmative obligations to keep the data confidential. The remainder of this section describes (1) utilities' obligations to protect customer usage data from unauthorized disclosures and (2) the circumstances under which law enforcement agencies and parties in civil litigation may compel utilities to produce meter data.

---

[69] "Loss" under the CFAA is expansive. It means "any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service." 18 U.S.C. § 1030(e)(11).

[70] 18 U.S.C. § 2511. "Interception" includes the activity of acquiring the contents of a communication in real time. This is the circumstance most directly related to the information flow described in the main text. But "interception" describes a broader range of conduct involving the acquisition of a communication's contents by a person who did not send a message and is not one of its intended recipients; "interception" is not limited to acquisition that is contemporaneous with transmission. The exact boundaries of "interception," however, remain unclear.

[71] CAL. PENAL CODE §§ 630-632.7.

[72] 18 U.S.C. § 2511(2)(g)(i).

These different stages of data flow from the smart meter to the utility raise an array of privacy issues, which we explore in the remainder of this section. Utilities in California are not subject to a specific, *statutory* requirement to keep information about customers confidential. This is in contrast to other entities that provide some of the same services as electric utilities. For example, electric service providers are required by statute to keep "customer information" confidential, unless the customer authorizes the release of information.[73] Similarly, telephone companies and Internet service providers are subject to a variety of federal and state restrictions on disclosing data to private parties and law enforcement agencies and other governmental entities.

California lacks analogous statutory rules for IOUs. IOUs operate under tariffs—"official rates and terms of service"[74]—that require them to keep customer information confidential. For example, PG&E promises not to "release confidential information, including financial information, to a third party without the customer's electronic signature or the [sic] written consent."[75] A CPUC rule requires investor owned utilities to obtain consent before sharing "customer information" with an "affiliate."[76] The CPUC has the authority to punish violations of utilities' own privacy rules[77] as well enforce its affiliate transaction rules.[78]

3.1.1.4 Protection Against Unauthorized Disclosures: Security Breach Notification Laws

IOUs—like other entities that do business in California and are thus subject to its security breach notification (SBN) law—must notify customers if "unencrypted personal information" about them "was, or is reasonably believed to have been, acquired by an unauthorized person."[79] SBN laws, however, have significant limitations where customer usage data from the

---

[73] CAL. PUB. UTILS. CODE § 394.4.

[74] CPUC, Utility Tariff Information, http://www.cpuc.ca.gov/PUC/energy/Electric+Rates/utiltariffs/ (last visited June 24, 2010).

[75] PG&E, Electric Rule 9 § M, (effective date Jan. 20, 2009), http://www.pge.com/tariffs/tm2/pdf/ELEC_RULES_9.pdf. *See also* PG&E, Opening Comments on Proposed Policies and Findings Pertaining to the Smart Grid, at 14 (Mar. 9 2010) (citing this tariff to support its argument that the Commission's existing customer privacy rules should be the basis of rules regarding third-party access to customer energy usage data and other customer-specific data").

[76] "Customer information" means "non-public information and data specific to a utility customer which the utility acquired or developed in the course of its provision of utility services." CPUC D. 97-12-088, revised by D.98-08-035 and amended by D.98-12-075. "'Affiliate' means any person, corporation, utility, partnership, or other entity 5 per cent or more of whose outstanding securities are owned, controlled, or held with power to vote, directly or indirectly either by a utility or any of its subsidiaries, or by that utility's controlling corporation and/or any of its subsidiaries." *Id.*

[77] The most obvious enforcement route would use the Commission's power to punish contempt: "Every public utility, corporation, or person which fails to comply with any part of any order, decision, rule, regulation, direction, demand, or requirement of the commission or any commissioner is in contempt of the commission, and is punishable by the commission for contempt in the same manner and to the same extent as contempt is punished by courts of record." CAL. PUB. UTILS. CODE § 2113.

[78] Violations of utility privacy rules might also be subject to punishment by the Federal Trade Commission, as discussed later in this report. *See infra* Part 3.d.i.

[79] CAL. CIV. CODE § 1798.82. Forty-six states and the District of Columbia have similar laws. Perkins Coie, Security Breach Notification Chart, http://www.perkinscoie.com/statebreachchart/chart.pdf (last visited June 22, 2010). Congress has considered, but has not passed, numerous bills that would create a

Smart Grid is concerned. A duty to notify applies only to breaches involving "personal information," which California's SBN law defines to mean an individual's name in combination with certain categories of information, such as an account number[80] Hour-by-hour traces of energy consumption are not among the categories of personal information listed in California's SBN. Unless an account number or other types of statutorily protected personal information accompany a breach of this information , it would not trigger a duty to notify affected customers.

3.1.1.5 Protection Against Compelled Disclosures

Like the unauthorized acquisitions of private information discussed above, certain types of lawful acquisitions can harm individual privacy. We discuss two scenarios of this type: law enforcement access and civil litigant access. Both involve a third party—a law enforcement agent or a civil litigant—compelling the production of private data from a utility. Though we presume the transfers that we discuss to be *lawful*, they nonetheless intrude upon individual privacy because they interfere with a person's ability to control information about him or her.

Law Enforcement Agencies.

CPUC rules do not regulate law enforcement access to data. The burden that a law enforcement agency must meet in order to obtain customer-specific data is unclear. One possibility is that customers have a reasonable expectation of privacy in the detailed record of in-home activities that meter data reveals, implying that law enforcement agents must obtain a warrant in order to gain access to the data.[81] One reading of the U.S. Supreme Court's ruling in *Kyllo v. United States*,[82] which involved infrared camera surveillance of individuals inside their own home, supports this view.[83] The CPUC has also interpreted California Supreme Court case law on the state constitutional right to privacy[84] to mean that law enforcement agents must obtain a search warrant or judicially issued subpoena before demanding utility customer records.[85]

---

federal security breach notification requirement. An "unauthorized person" may have obtained access either through accident (e.g., a misconfigured website) or a malicious attack. California's SBN law requires notification under both circumstances.

[80] CAL. CIV. CODE § 1798.82(e).

[81] For an argument in favor of this view, see Joint Comments of Center for Democracy & Technology and the Electronic Frontier Foundation on Proposed Findings and Policies Pertaining to the Smart Grid 10-12 (filed with CPUC, Mar. 9, 2010).

[82] 533 U.S. 27 (2001).

[83] *See* Jack I. Lerner & Deirdre K. Mulligan, *Taking the 'Long View' on the Fourth Amendment: Stored Records and the Sanctity of the Home*, 2008 STAN. TECH. L. REV. 3.

[84] CAL. CONST., art. I, §§ 1, 13.

[85] CPUC, Opinion Denying Petition of California Narcotic Officers' Association to Modify Decision 90-12-121, D.01-07-032, Jul. 12, 2001; *see also* Joint Comments of the Center for Democracy and Technology and the Electronic Frontier Foundation on Proposed Policies and Findings Pertaining to the Smart Grid, at 31-33, R.08-12-009, Mar. 9, 2010 (discussing CPUC Decision 01-07-032 and the underlying line of cases) ["CDT/EFF Opening Comments"].

As the *CyberKnowledge/Berkeley Report* points out, however, a second possibility is that law enforcement agents may simply *request* a customer's meter data.[86] The California Court of Appeals has held that utility records are business records that are voluntarily handed over to a third party, and thus devoid of a reasonable expectation of privacy.[87] Federal courts have reached the same conclusion.[88]

Between these two extremes is a third possibility: that law enforcement agents must present a grand jury subpoena, which is quicker than a judge-issued subpoena and does not involve the oversight of a neutral decision-maker.[89] This appears to be the common practice among law enforcement officials in California.[90]

Given the increased details that smart meter data may reveal, it remains to be seen whether the CPUC, California courts, or the California legislature will close these gaps and clarify the law. It is clear, however, that any of these branches of government have significant latitude to set rules regulating law enforcement agencies' access to meter data.

Civil Litigants. Meter data is available to litigants in a civil case on relatively easy terms. A party in a civil suit—such as a divorce, where meter data could be highly relevant—may obtain the data from an IOU with a subpoena.[91] Neither the utility nor the party issuing the subpoena needs to notify the individual(s) whose activities are reflected in this data. This significantly limits the opportunity of the customer to assert a privacy interest and object to the subpoena.

Again, the contrast to other domains involving detailed data about individual activities is striking. For example, in California, in the financial, insurance, and health care domains, individuals must be given an opportunity to object to subpoenas demanding their personal information.[92] Subpoenas for telephone records contain an extra procedural safeguard: they must be signed "by the consumer whose records are requested" in order to be valid.[93]

3.1.2 Energy Usage Information Collected by a Customer-Owned Metering Device

A significant shift in the Smart Grid, relative to its predecessor, is that it will enable entities other than utilities—third parties—to collect meter data. Smart grid data can be obtained either

---

[86] *CyberKnowledge/Berkeley Report*, *supra* note 3, at 25 (discussing Cal. Penal Code § 1326.1(e), which states that "[n]othing in this section shall preclude the holder of the utility records from voluntarily disclosing information or providing records to law enforcement upon request").

[87] People v. Stanley, 72 Cal. App. 4th 1547, 1552-54 (2d App. Dist. 1999); *CyberKnowledge/Berkeley Report*, *supra* note 3, at 26-27.

[88] *See* United States v. Starkweather, 1992 U.S. App. LEXIS 20207 (9th Cir.); CyberKnowledge/Berkeley Report, *supra* note 3, at 26 (discussing cases).

[89] *See CyberKnowledge/Berkeley Report*, *supra* note 3, at 30-31 (noting that an investigator may obtain a grand jury subpoena "can be done in as little as ten minutes").

[90] *See CyberKnowledge/Berkeley Report*, *supra* note 3, at 30-31 (reporting, based on interviews with current and former U.S. Attorneys, that investigators typically use grand jury subpoenas in non-emergency situations, in part because utilities typically decline to produce customer records voluntarily).

[91] CAL. CODE CIV. PROC. §§ 2010.410-2020.440.

[92] CAL. CODE CIV. PROC. § 1985.3(a), (c).

[93] CAL. CODE CIV. PROC. § 1985.3(f).

from the utilities or directly from the individual's network or devices. This section considers the privacy issues arising when data is obtained directly from individuals.

Individuals may purchase[94] their own metering devices and use them to send data entirely separately from utility-owned infrastructure. Figure 3. Currently, these devices cost from $20 to $200.[95] Alternatively, individuals may choose to use devices, such as The Energy Detective (TED). TED uses current transformers (CTs) to measure electricity consumption; basically, two clips placed around the electrical wires entering a home's circuit breaker measure how much electricity flows into the house. The device uses this connection to measure electricity consumption at one-second intervals when the CTs are attached to breaker panels.[96] TED devices can also connect to the Internet and send energy usage information to third parties who may, in turn, present analyzed data via cell phone or Web-based applications.[97]

The devices that customers buy on their own may measure electricity usage at both device and household levels. (Figure 3 shows device-level measurements.) For instance, customers may have end-use metering to support distributed generation, or monitor discreet loads.[98]

[94] Presumably customers will also be able to lease, rent, or use a third-party-provided metering device. We use the term "customer-owned metering device" to describe all of these cases, the common thread being that the metering device is not the utility meter.

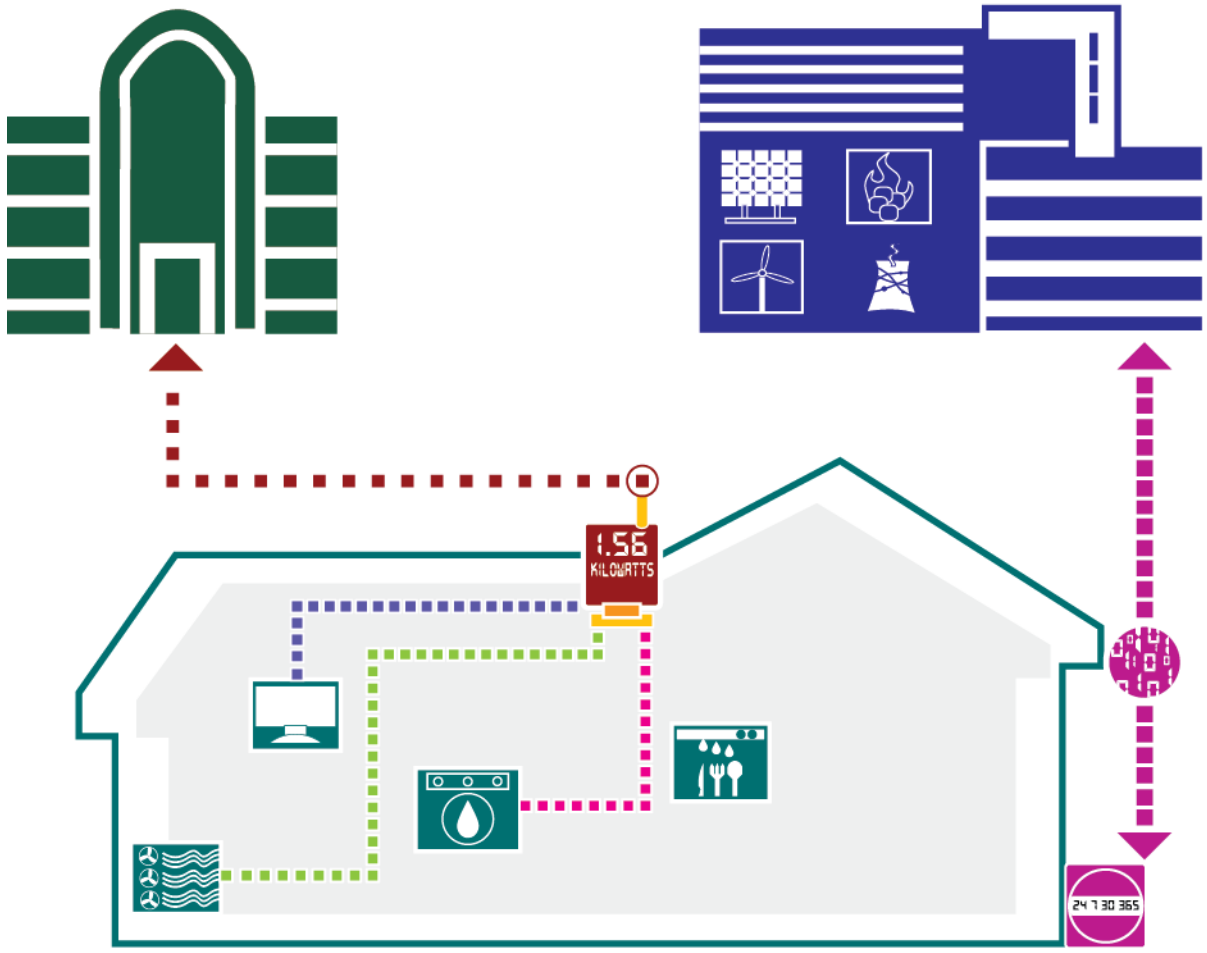
[95] ChooseRenewables, Energy Usage Monitors, https://www.chooserenewables.com/xcart/home.php?cat=266&gclid=CLXXlOyHo6ECFQ8bawodWBiSww (last visited June 20, 2010) (showing a list of energy usage monitors that customers can purchase).

[96] TED, How Do I Install TED?, http://www.theenergydetective.com/about-ted/how-do-i-install-ted (last visited June 20, 2010); TED, Measuring Transmitting Unit (MTU) and Current Transformers (CTs), http://www.theenergydetective.com/which-ted.html.

[97] TED, Third Party Applications for TED 5000, http://www.theenergydetective.com/ted-5000/3rd-party-apps (last visited June 20, 2010).

[98] ZigBee Alliance and HomePlug Powerline Alliance, *Smart Energy Profile 2.0 Technical Requirement Document v0.5* at 57 ("end-use metering that includes additional meters installed in the premises to support distributed generation production or measurement of discreet loads.") ["SEP 2.0 Technical Requirement Document v0.5"]

Figure 3: Meter data collected by customer-owned meter



A customer-owned metering device (at the top of the house) measures electricity consumption and other data, and sends the data over a general-purpose network (e.g., the Internet or a cellular network) to a third party (drawn in green in the upper left-hand corner of the figure) for collection and analysis. The third party might provide services such as presenting analyzed data or sending energy usage alerts to the customer. The utility-owned meter sends similar data to the utility over its own network, though the measurement interval and uses of data may be different.
Graphics Credit: Brian P. Miller Photo & Design, http://www.brianpmillerphotography.com/

The differences in the device-specificity of usage information, the frequency with which energy usage data is measured and transmitted, and the potentially wide variety of third-party data recipients create a complex set of privacy issues. Data from the customer-owned metering device might not be transferred to or from the utility (though the utility will obtain data from its own meter); this could leave data from the customer's metering device beyond the scope of CPUC regulations. The CPUC has considered privacy rules to govern third-party access to customer usage data, but it has not adopted a final rule.[99]

[99] As the CPUC explains, "privacy protections and the reach of Commission jurisdiction are under review by legislation pending before the State Legislature. Legislative action may provide greater legal clarity in

Even if the CPUC (and utilities commissions in other states) do not regulate third parties, the data they handle will be subject to more general legal protections. For example, the general—but limited—protections offered by the federal Electronic Communications Privacy Act (ECPA), the Federal Trade Commission (FTC) Act, and state security breach notification laws still apply.[100] As discussed in the next section, ECPA imposes few limits on how authorized recipients of meter data may use it, and it is questionable whether its protections against disclosure to law enforcement agencies apply to utilities and third parties that might handle this data. The FTC Act applies to a broad range of "unfair" or "deceptive" conduct that gives rise to privacy harm, but enforcement has been rare in cases in which a firm gives adequate notice of its data processing practices. Finally, security breach notification laws require firms to give notice after discovering unauthorized access to certain categories of personally identifiable information. As discussed above, however, as breach notification laws may not apply to many breaches.

Overall, customer-owned metering devices are not subject to the same level of public or regulatory review as utility-owned devices prior to going on the market. Moreover, the laws that do apply to third parties omit many FIPs, by failing to require third parties to specify the purposes for data collection, minimize data collection to what is necessary to achieve these purposes, and limit actual uses to the stated purposes. It remains to be seen whether utilities regulators, state legislatures, or other authorities will develop rules that are tailored for customer usage data.

3.1.3 Third Party Access to Energy Usage Information Held by Utilities

This section discusses the acquisition of energy usage information from utilities by third parties, as shown in Figure 4. This section also highlights that the applicable privacy laws, and privacy regulators, change dramatically as information travels from the customer, to the utility, to one or more third parties.

3.1.3.1 Third party Access Via a Utility

Enabling this kind of information flow is a major priority of Smart Grid policy. Though San Diego Gas and Electric (SDG&E) and Sacramento Municipal Utility District (SMUD) are the only California utilities with programs in place to provide data to third parties, the CPUC is requiring all major IOUs to provide consumers and third parties approved by consumers with

---

this matter. If there is no action on this matter by the Legislature, then the Commission will consider inviting legal briefs to clarify the extent of the Commission's jurisdiction and to recommend the best procedure for protecting consumer interests." Decision Adopting Requirements for Smart Grid Deployment Plans Pursuant to Senate Bill 17 (Padilla), Chapter 327, Statutes of 2009, at 43 n.90, CPUC R.08-12-009, June 28, 2010.

[100] *See* the discussion in Part 3.2.3 below.

usage data by the end of 2010.[101] The CPUC proposed rules to govern third-party access to energy usage information, but as of this writing it has not adopted final rules.[102]

Two prominent third-party energy usage information-processing services—Google PowerMeter and Microsoft Hohm—are similar in overall design, though they have some underlying technical differences. Most importantly, both services obtain energy usage information directly from utilities, but only when customers choose to use the service. Utilities do not provide the information to Google or Microsoft without the customer's consent.

To enroll in Google PowerMeter, users first authenticate themselves on the utility website, and then use the utility website to authorize Google PowerMeter to access their energy usage information.[103] Google assigns each PowerMeter user a unique PowerMeter ID.[104] The utility provides energy usage information to PowerMeter at 15-minute to hourly intervals, depending on the utility.[105] The information is transferred to Google via an encrypted connection in a data format specified by Google.[106] The information transfer is associated with the PowerMeter ID; customers do not need to provide Google Account username to the utility for the data transfer, nor do customers provide their utility account number to Google.[107] Once the energy usage information is stored with PowerMeter, users can log in with Google Account username to view

---

[101] CPUC Decision 09-12-046 (Dec. 17, 2009) at 3 ("Concerning electricity usage data, we require that SCE, PG&E and SDG&E provide consumers and third parties approved by consumers with usage data that is collected by the utility by the end of 2010.").

[102] Assigned Commissioner and Administrative Law Judge's Joint Ruling Amending Scoping Memo and Inviting Comments on Proposed Policies and Findings Pertaining to the Smart Grid, Attachment B, CPUC R.08-12-009, Feb. 8, 2010, http://docs.cpuc.ca.gov/efile/RULINGS/113482.pdf.

[103] Google PowerMeter, Enrollment, http://sites.google.com/site/powermeterpartners/enrollment (last visited June 20, 2010).

[104] Google, Google PowerMeter API Data Model, http://code.google.com/apis/powermeter/docs/meter_api_datamodel.html (last visited June 20, 2010) ("The Google PowerMeter ID is a unique, 20-digit ID representing a user. The ID is issued when the user consents (on the Google PowerMeter web site) to Google PowerMeter program terms. To protect user privacy, the generated ID is specific to Google PowerMeter and cannot be linked to other Google service IDs for the same Google account. For more information, refer to the description of the device activation process.")

[105] Google, Google PowerMeter Privacy Policy Notice, http://www.google.com/powermeter/privacy (last visited June 20, 2010) ("The frequency of these readings depends on your utility; for example, some utilities will send hourly readings, others will send fifteen (15) minute interval readings throughout the day."). Since utilities in California collect hourly data from residential customers, they cannot provide more fine-grained data.

[106] Google, Google PowerMeter API Data Model, http://code.google.com/apis/powermeter/docs/meter_api_datamodel.html (last visited June 20, 2010).

[107] Google, Google PowerMeter Privacy Policy Notice, http://www.google.com/powermeter/privacy (last visited June 20, 2010) ("Google creates a unique PowerMeter user identifier at the time of enrollment in your utility's PowerMeter program. All data sent by your utility to Google will be tagged with this unique identifier only.")

their information. Users can also choose to share their information with other PowerMeter users, on an opt-in basis.[108]

Microsoft Hohm adopts a different authentication process.[109] A utility partnered with Hohm first provides three authentication questions to Hohm. After a utility customer answers these questions on Hohm website, Hohm provides the answers to the utility to authenticate the customer. If the authentication is approved by the utility, Hohm generates a customer ID and provides it to the utility. The utility then provides the customer's energy usage information associated with the customer ID to Hohm in the XML format defined by Microsoft.

To address the problem that different third parties have their own formats for customer data, major California IOUs, Microsoft, Google, and others have proposed Open Automated Data Exchange (OpenADE) to standardize energy usage information exchange between utilities and third parties.[110] NIST is also coordinating a working group to develop standards for the exchange of energy usage information.[111]

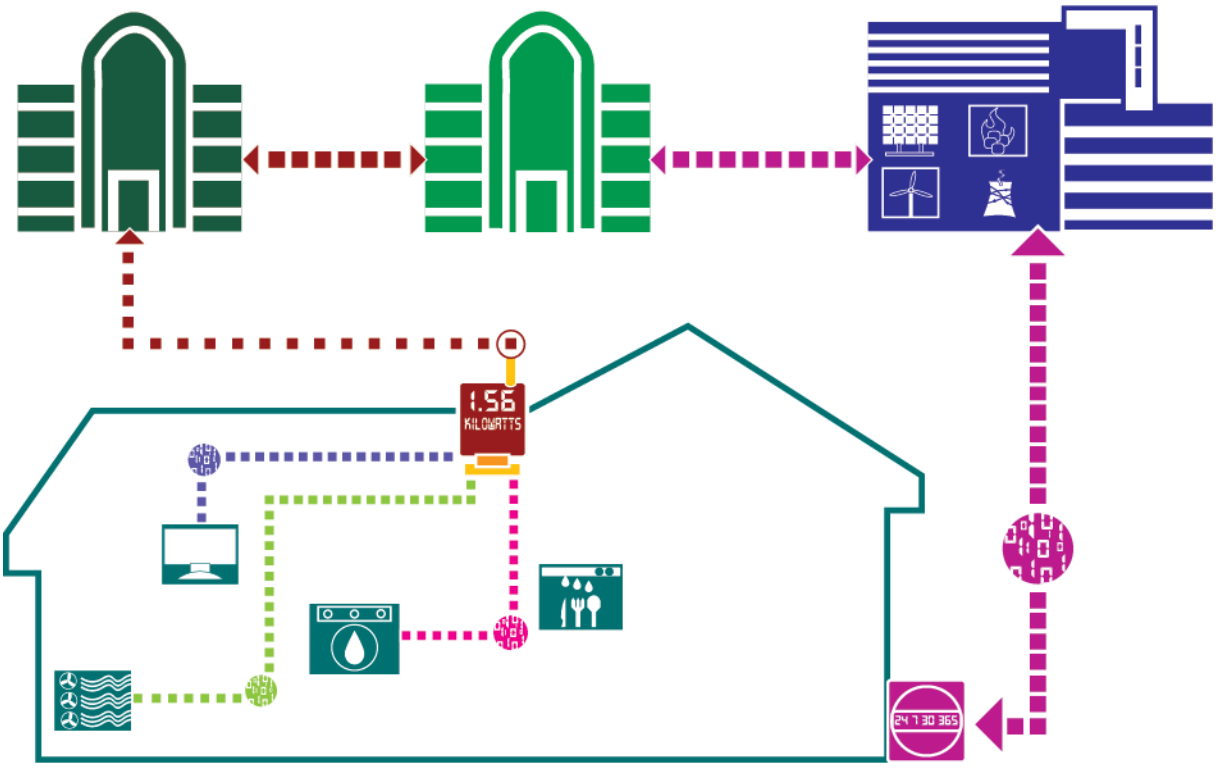
Figure 4: Energy usage information flow patterns involving third parties

[108] Danan Sudindranath, Share your Power(Meter)!, http://blog.google.org/2010/03/share-your-powermeter.html (last visited June 20, 2010).

[109] Microsoft, Integrating with Hohm – Registering Customers, http://msdn.microsoft.com/en-us/library/ee724246(v=MSDN.10).aspx (last visited June 20, 2010).

[110] UCAIug OpenSG OpenADE Task Force, *OpenADE 1.0 System Requirements Specification,* http://www.smartgridipedia.org/images/0/0e/OpenSG_OpenADE_1.0_SRS.pdf (last visited June 20, 2010); *OpenADE Charter*, http://www.smartgridipedia.org/index.php/OpenADE_Charter (last visited July 17, 2010) (stating that price information will be included in OpenADE 2.0).

[111] NIST, *NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0* 79, NIST Special Publication 1108, http://www.nist.gov/public_affairs/releases/upload/smartgrid_interoperability_final.pdf ("Subsequent work in the first half of 2010 will drive a standardized information model for broader exchange of usage information.").



Third parties may obtain energy usage information in several ways: from a utility, from another third party, or directly from a customer-owned meter.
Graphics Credit: Brian P. Miller Photo & Design, http://www.brianpmillerphotography.com/

Some of the privacy risks associated with energy usage information transfers from utilities to third parties are now familiar: The information may be disclosed law enforcement agencies or civil litigants, as discussed in section 3.2.1. In addition, third parties' business reasons for collecting the information may differ from those of utilities. Non-utility third parties may have economic incentives to use or share customer's energy usage information, for example, as part of marketing campaigns.[112] Third parties may also say little about what information they collect and use, and their disclosures may be in the form of lengthy, impenetrable privacy policies. All of these factors may make it difficult for customers to understand the effects of agreeing to information disclosures.

As discussed below, consumer protection agencies such as the Federal Trade Commission have imposed few substantive requirements on privacy policy disclosures, though recent enforcement actions may signal a change in approach.[113] Furthermore, customers who seek to understand the information privacy practices of several competing third-party service providers will need to review each company's privacy policy. Given how these documents are

[112] *See* CDT/EFF Joint Opening Comments, *supra* note 54, at 26 ("Some third parties seeking access to customer data are likely to have business models based upon offering the consumer a service, perhaps for free, and then commercializing and selling the data.").

[113] *See* Wendy Davis, *Sears Required To Destroy Tracking Data*, Online Media Daily, Sept. 9, 2009 (quoting sources who opined that the *Sears* settlement marked a new disclosure standard at the FTC).

typically written, this would likely involve a significant investment of time and effort.[114] Still, provided that privacy policies are publicly available, some individuals or entities (e.g., nonprofits) may be willing to analyze and compare them.[115]

Public Utilities Commission Regulation of Third Parties. Third parties that obtain customers' energy usage information from utilities may be subject to two very different privacy regimes. First, by virtue of their dealing with utilities, they may be subject to indirect CPUC regulation. That is, the CPUC could require investor owned utilities to impose certain conditions on their third-party partners. In addition, the CPUC may adopt an access rule that directly regulates third party use, retention, and protection of customers' energy usage information.[116] As stated above, however, the CPUC has not adopted a final rule on this topic.

Applying General Data Privacy Laws to Third Parties. Irrespective of whether utilities regulators adopt privacy rules for third parties, they are subject to general state and federal data privacy and security laws. As discussed in section 3.2.1, these include:

- Criminal prohibitions on obtaining data by intercepting it or hacking into the third party's computers;
- Security breach notification laws, which require a third party to notify customers in the event of unauthorized access to personally identifiable information.
- Subpoena requirements for law enforcement agency and civil litigant access to data.

These restrictions are obviously limited in scope. Tariff rules provide some privacy protection by stating that the utility will not release "confidential information" to a third party—which, stated without qualification, includes private parties and governmental entities—without customer consent.[117] Amending tariffs to reduce these protections, however, is far easier than

---

[114] There are, of course, exceptions. *See, e.g.*, Google, Google PowerMeter Privacy Policy Notice, http://www.google.com/powermeter/privacy (last visited June 8, 2010).

[115] *See* Aleecia M. McDonald, Robert W. Reeder, Patrick Gage Kelley, and Lorrie Faith Cranor, A Comparative Study of Online Privacy Policies and Formats, Privacy Enhancing Technologies Symposium, Aug. 5-7 2009, draft available at http://www.aleecia.com/authors-drafts/PETS-formats-AV.pdf.

[116] *See, e.g.*, Joint Comments of Center for Democracy & Technology and the Electronic Frontier Foundation on Proposed Findings and Policies Pertaining to the Smart Grid, at 26, CPUC R.08-12-009 (Mar. 9, 2010) ("We support the Commission's suggestion to require customer authorization before a utility provides customer data to any third party. However, given the highly personal nature of the data that would potentially be shared, the Commission should adopt a strong privacy standard in its Proposed Access Rule and should condition access on requirements that follow the Fair Information Practice principles.") (internal citation omitted); Reply Comments of Google Inc. on Proposed Policies and Findings Pertaining to the Smart Grid 5, CPUC R.08-12-009, Apr. 7, 2010 (endorsing the idea of using utility-third party service agreements to harmonize their customer usage data policies). *But see* SCE Reply Comments at 21 (urging "the Commission [to] reject any proposal that imposes on the utility a duty to enforce the compliance of customer-authorized third parties with state and federal privacy laws in their use of customer data" and stating that "[t]he utility does not enter into contracts with customer-authorized third-party agents, as some parties appear to have incorrectly assumed").

[117] *See, e.g.*, PG&E Electric Rule 9, ¶ M (filed Aug. 4, 2006).

amending statutes or regulations. Moreover, none of these constraints on *disclosures* to third parties address the significant privacy issues stemming from third parties' internal *uses* of the information. Nor do they limit third parties' disclosures to other third parties, whether they are private or governmental entities. Generally speaking, federal and state laws place few restrictions on how the usage information can be used and with to whom it may be disclosed.

Protection for Customers' Energy Usage Information Under Consumer Protection Laws. Perhaps the most general data privacy framework comes from the Federal Trade Commission. Beginning in the mid-1990s, the FTC has used its authority to police "unfair or deceptive acts or practices" [118] to investigate and enjoin online practices that harm consumer privacy interests. The FTC may issue general rules "which define with specificity acts or practices which are unfair or deceptive acts or practices"[119] once it believes that such practices are "prevalent."[120] In the context of information privacy, the FTC has drawn attention to a limited set of FIPs: (1) notice/awareness; (2) choice/consent; (3) access/participation; and (4) integrity/security.[121] Failing to disclose, or making deceptive statements about, how information will be used or shared may be "deceptive" acts. If consumers cannot reasonably avoid these practices and do not receive countervailing benefits, the practices may be deemed "unfair."[122]

Many commentators have criticized the FTC for focusing on notice and consent, to the exclusion of other information privacy principles that bear on Section 5.[123] As discussed in section 2.3, a full set of FIPs emphasizes the importance of specifically stating the purposes for data collection, as well as limiting data collection, use, and retention to what is necessary to fulfill these purposes. To oversimplify a bit, the common wisdom has been that making a broad (or vague) disclosure of information practices would insulate a company from FTC action.

Recent FTC enforcement activity, however, suggests that it may begin to take a more substantive look at the data collection and use practices that are covered by a given notice. Specifically, the FTC filed a complaint against Sears for conducting a marketing campaign that depended in part on installing an application on users' computers.[124] The application was capable of monitoring all Internet traffic—not just traffic between a user's computer and Sears—

---

[118] 15 U.S.C. § 45.

[119] 15 U.S.C. § 57a(a)(1)(B).

[120] 15 U.S.C. § 57a(b)(3).

[121] FTC, *Privacy Online: Fair Information Practices in the Electronic Marketplace* 4 (2000); *see also* Center for Democracy & Technology, Comment for FTC's Privacy Roundtable 6-7 (Nov. 2009) (critiquing this version of FIPPs as too narrow).

[122] *See* 15 U.S.C. § 45(n) (defining scope of FTC's "unfairness" jurisdiction).

[123] *See* Center for Democracy & Technology, Comment for FTC's Privacy Roundtable 9 (Nov. 2009) (criticizing FTC for adhering to an "opt in/opt out consent paradigm [that] at best only gives consumers control over their data at the point of collection"). More broadly, a Department of Commerce official stated that "'[t]here are essentially no defenders anymore of the pure notice-and-choice model.'" Steve Lohr, *Redrawing the Route to Online Privacy*, N.Y. TIMES, Feb. 28, 2010, *at* Bus. 4 (quoting National Telecommunications and Information Administration Associate Director for Domestic Policy Daniel J. Weitzner).

[124] *See* In the Matter of Sears Holdings Management Corporation, Complaint, FTC File No. 082 3099, *at* http://www.ftc.gov/os/caselist/0823099/index.shtm.

and transmitting reports to Sears. Though the FTC alleged in its complaint that Sears did not describe in sufficient detail the scope of this application's traffic monitoring, and thus stayed within the notice-and-consent paradigm, this action may signal that the FTC will require notices to be more specific about how a firm collects and uses data, even if it does not disclose the data to other organizations. The FTC has also emphasized that "there are occasions when disclosure in a EULA [end-use license agreement] may not be sufficient to correct a misleading impression created elsewhere."[125] That is, the overall impression that a company gives about its data collection and use practices matters.

In addition, state-level "mini FTC Acts" authorize state attorneys general (or state consumer protection authorities, or both) to sue to enjoin unfair or deceptive trade practices. California Business & Professions Code § 17200, for example, authorizes government lawsuits to enjoin or seek damages from any person or business that engages in an "unfair business act or practice."

Consumer protection law does not represent a complete approach to protecting customers' energy usage information. The strengths of the FTC's approach to data privacy in the broader context of electronic commerce have been that it allowed business practices and consumer expectations of privacy to evolve; instead of encouraging compliance with clear but static rules, the FTC has encouraged companies to evaluate and re-evaluate their information practices.[126] Yet, the Smart Grid context is distinct in several ways that counsel for more clearly articulated rules. First, Smart Grid infrastructure is nascent and provides an opportunity for utilities, regulators, device vendors, service providers, and consumers to design privacy-protecting features into devices and services.[127] Second, the privacy risks of third-party handling of customers' energy usage information are evident, removing one of the underpinnings for the ambiguity that has marked FTC enforcement. Finally, it remains uncertain whether the FTC will follow the direction suggested by the *Sears* case and move toward more substantive review of privacy policies. Instead, the FTC may abstain from enforcement in this area to devote its limited resources to other, higher-priority industry sectors and for a host of other substantive and political reasons.

Protection for Customers' Energy Usage Information Under Communications Privacy Law. Another potential restriction on a third party's ability to redistribute customer usage data is the Stored Communications Act (SCA), which is a part of the Electronic Communications Privacy Act (ECPA).[128] Of particular relevance here is the SCA's prohibition on a provider of a "remote computing service [RCS] to the public" from knowingly disclosing the contents of an electronic communication that is "maintained on that service . . . solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not

---

[125] Letter from Federal Trade Commission to Alan Charles Raul, Aug. 31, 2009, http://www.ftc.gov/os/caselist/0823099/090909searsletteraustin.pdf.

[126] *See* Kenneth A. Bamberger & Deirdre K. Mulligan, *Privacy on the Books and on the Ground*, 63 STAN. L. REV. (forthcoming 2011).

[127] *See* The Future of Privacy Forum & Information and Privacy Commissioner of Ontario, *SmartPrivacy for the Smart Grid: Embedding Privacy into the Design of Energy Conservation* 12-17, Nov. 2009 (posing privacy-related questions pertaining to Smart Grid components and entities).

[128] The SCA was enacted as Title II of the Electronic Communications Privacy Act of 1986 (ECPA), Pub. L. 99-508, and codified at 18 U.S.C. §§ 2701 *et seq.*

authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing."[129] As the U.S. Department of Justice has stated in an official document, "[r]oughly speaking, a remote computing service is provided by an off-site computer that stores or processes data for a customer."[130]

A provider of an RCS to the public is subject to two kinds of restrictions. First, it may not divulge non-content *records* pertaining to a customer to a "governmental entity"[131] without a court order or subpoena.[132] The RCS provider may disclose these records to any private party. Second, the RCS provider may not divulge the *contents* of communications, unless presented with a valid court order or subpoena.[133] Of the several exemptions that apply to these general rules, the most important is customer consent, which we discuss below.

The third parties described in this section could fall under the SCA's restrictions. They appear to meet the basic definition of RCS because they provide "computer storage or processing services by means of an electronic communications system" to the public.[134] Moreover, these services both store data transferred from utilities on behalf of the utility customer and offer "computer processing services." Whether the Smart Grid services discussed in this section have access to communications *only* "for purposes of providing . . . storage or computer processing" is a closer question. The answer depends on a specific third party's terms of service and privacy policy. The privacy policy for Google PowerMeter, for example, states that "Google may share your anonymous, aggregated electricity consumption information with other PowerMeter users, PowerMeter partners, or through an API available to developers."[135] Google's policy appears to allow it to access data in PowerMeter accounts, which might render ECPA's RCS restrictions inapplicable.[136]

---

[129] 18 U.S.C. § 2702(a)(2)(B).

[130] U.S. Dept. of Justice, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations* 119 (2009).

[131] The definition of "governmental entity" includes, but is broader than, law enforcement agencies.

[132] 18 U.S.C. § 2702(c).

[133] Depending upon the process used, notice may or may not be required. For a discussion of the options for law enforcement access, see Kerr, Orin S., A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It. George Washington Law Review, 2004.

[134] An "electronic communications system" is "any wire, radio, electromagnetic, photooptical or photoelectronic facilities for the transmission of wire or electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications." 18 U.S.C. § 2510(12).

[135] Google, PowerMeter Privacy Policy, http://www.google.com/powermeter/privacy (last visited May 18, 2010).

[136] The SCA's restrictions on a remote computing service's disclosure of communications apply only if the service "provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing." 18 U.S.C. § 2702(a)(2)(B). A service that is authorized to access communications—even for the purpose of processing them to render them "anonymous," as in Google's case—might not fit this narrow description.

Even if the SCA's disclosure restrictions to third-party energy usage information processors, customer consent provides a way around them. If the "subscriber" of an RCS gives "lawful consent," the RCS provider may disclose records pertaining to the subscriber (name, address, subscriber identification, and network connection information[137]), as well as the contents of the subscriber's communications.[138] Exactly how expansive consent may be is unclear.[139] In other electronic surveillance contexts, such as wiretapping, courts have sometimes found notice of monitoring in an organization's official policies (such as its terms of use) to be sufficient to establish consent to real-time monitoring of communications.[140] If analogous interpretations of consent apply in the context of the SCA and customers' energy usage information, a general statement of consent could permit the disclosure of data to private parties, law enforcement agencies, and other government agencies.

Thus, protection for stored customer information under federal communications privacy law is uncertain. Case law sheds little light on what kinds of services meet all elements of the statute's definition, and relatively minor changes in the design of a service, and the policies governing the service provider's use of data, could eliminate the disclosure protections that may have applied.

3.1.3.2 Access Via a Customer-Owned Device

Customer-owned devices may provide energy usage information directly to third parties. As explained in sections 3.2.2 and 3.2.4, a customer device may obtain the information either from a smart meter via a HAN gateway, and transmit this data to a third party; or a customer-owned metering device could provide its own measurements of energy usage information. For instance, Google PowerMeter already provides an application programming interface (API) that allows any device that meets a set of predefined requirements to send data directly to PowerMeter via the Internet. In addition, customer devices may simultaneously provide energy usage information to multiple third parties. The Energy Detective (TED), discussed above, makes its own API available to third party developers. Using the TED API, customer usage data recorded by TED can be sent to third parties that communicate with TED, such as Google PowerMeter, iPhone applications, home automation systems, etc.

The most significant change in this information flow, relative to a third party obtaining a customer's energy usage information from a utility (section 3.2.3.1), is that utilities commission

---

[137] 18 U.S.C. § 2703(c)(2).

[138] 18 U.S.C. § 2702(b)(3) (providing consent exemption for disclosure of communications *contents*); *id.* § 2702(c)(2) (providing consent exemption for disclosure of communications *records*). A further subtlety here is that the SCA requires the consent of the "subscriber of the remote computing service." 18 U.S.C. § 2702(b)(3). In the context of this information flow, this "subscriber" is likely the person who signs up for an account with a third-party service. In some situations, such as an owner-occupied home, this subscriber will also be the electric utility account holder. But in many situations—an apartment building in which the landlord holds the utility account, for example—they may differ.

[139] One clear limit is that consent obtained by deception is not valid. *See* Theofel v. Farey-Jones, 359 F.3d 1066, 1073-75 (9th Cir. 2004). *See also* Orin S. Kerr, *A User's Guide to the Stored Communications Act*, 72 GEO. WASH. L. REV. 1208, 1224-26 (2004) (discussing the lack of case law interpreting the SCA's consent exemptions).a

[140] *See* U.S. Dept. of Justice, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations* 48-50 (2009).

jurisdiction is tenuous. The protections—and gaps in protection—from consumer protection law and the ECPA, however, are basically unchanged.

3.1.3.3 Access Via a Third Party

Figure 5 also illustrates that energy usage information may be transferred from one third party to another. For instance, Google PowerMeter permits users to share their information with other PowerMeter users. Data sharing among third parties could become more extensive in the future. For example, a third-party collection and processing service could send energy usage information to down-stream third-party developers, such as start-up energy management companies.

As section 3.2.3.1 suggests, a primary source—and limitation—of privacy protection in this information flow is the notice that the initial third party provides to customers. The statements in these privacy policies are backed by the threat of FTC or state attorney general enforcement if notice is deficient, or actual practices deviate from the notice.

3.1.4 Energy Usage Information from Smart Meter to HAN

The Smart Grid also supports the increased flow of information to individual customers. Indeed, one of the premises of state and federal Smart Grid policy is that providing customers with timely information about their energy use will lead them to use less energy or use it more efficiently. Adding price information provides a potentially powerful way of motivating customers to alter their usage patterns and enabling automated, price-responsive energy management.

Figure 5 shows how customers might acquire energy usage information in real time. The information flow in this Figure is mostly local; consumption and other data measured by the smart meter are routed through the HAN gateway to and in-home display or devices in the home. The purpose of enabling direct smart meter-to-HAN information flow is to eliminate the bottleneck that would arise from transmitting real-time information from the meter, to the utility, and then back to the customer. Smart meters can measure electricity consumption at short intervals, roughly every 10 seconds.[141] Transmitting such fine-grained data to the utilities would overwhelm the capacity of their backhaul networks, but home area networks do not suffer from such severe resource constraints.[142] Therefore, sending data directly from a smart meter to the HAN appears to be a more feasible way of providing customers with real-time information; but using utility backhaul networks for this purpose does not.

---

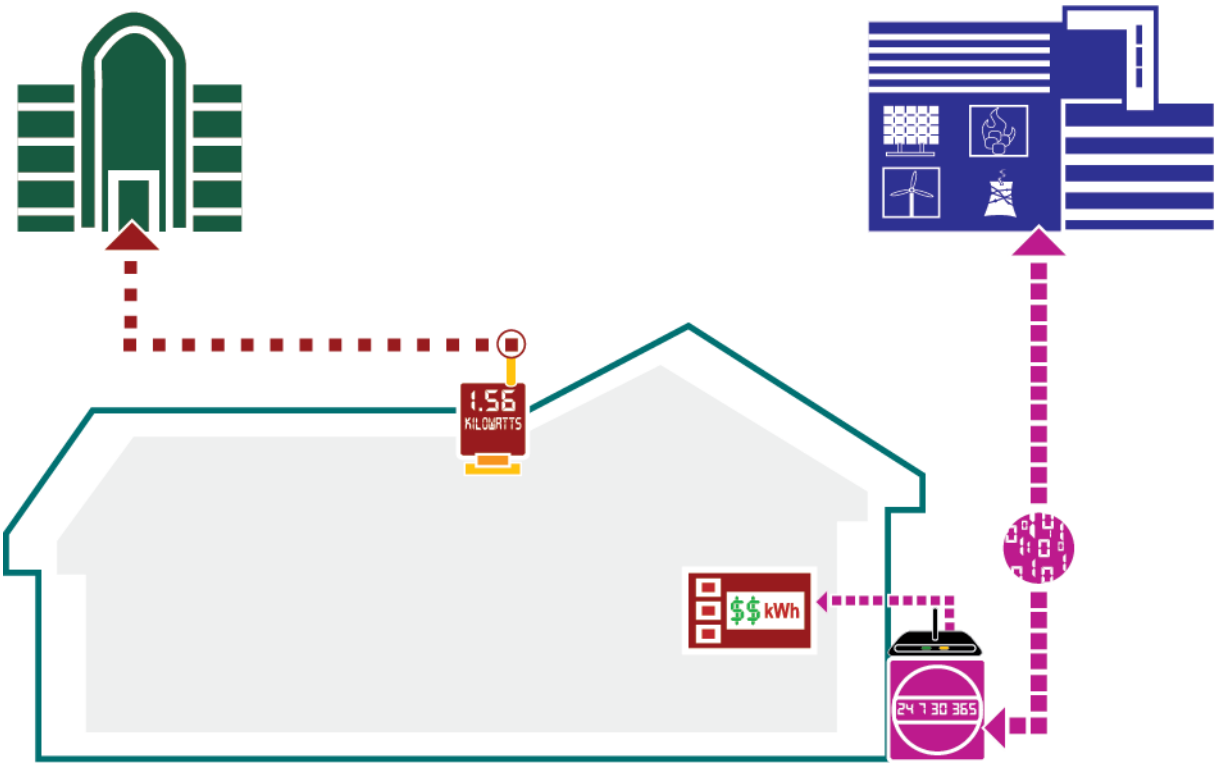
[141] SCE, Reply Comments to Assigned Commissioner and Administrative Law Judge's Joint Ruling Amending Scoping Memo and Inviting Comments on Proposed Policies and Findings Pertaining to the Smart Grid 14, R.08-12-009, Apr. 7, 2010, http://www.cpuc.ca.gov/EFILE/CM/115972.pdf. ("[T]he Commission also decided that it is reasonable to provide residential customers with near real-time usage data through the HAN. Accordingly, SCE, PG&E, and SDG&E have plans to provide near real-time usage data, in approximately ten-second increments, to all residential customers.")

[142] Opening Comments of Pacific Gas and Electric Company (U 39 E) on Proposed Policies and Findings Pertaining to the Smart Grid, at 15, CPUC R.08-12-009, Mar. 9, 2010 ("'Real time access' to customer usage and pricing information can only come from localized access to such information through a Home Area Network device at the customer's premises—*not* from utility 'back office' data collection and communication facilities.").

The CPUC has granted approval for all three major IOUs to recover the cost of embedding a HAN gateway in their smart meters. When activated, the HAN gateway will route energy usage information from the smart meter to HAN devices that display electricity usage information to customers. The CPUC's rationale for allowing HAN gateways to be part of smart meter deployment, rather than leaving it to customers to decide whether to purchase their own HAN gateway, is that "all customers should have the opportunity to use HAN devices to reduce their energy consumption," and the "most cost effective way to provide that access, over the long term, would be through . . . meter deployment plan rather than through random retrofits." The CPUC has scheduled the activation of the HAN gateway in smart meters to be no later than the end of 2011.[143]

[143] CPUC Decision 09-12-046 at 65 (requiring that "each IOU be capable of providing a customer with an AMI meter with access to the customer's usage information on a near real-time basis by the end of 2011 should the customer desire that information").

Figure 5: Energy usage information flow on the home area network



A HAN gateway, shown as the black device attached to the smart meter, sends energy usage information to an in-home display. The display, in turn, presents real-time energy consumption and price information to the customer. This short-interval data (~10 seconds between measurements) goes from the HAN gateway to the in-home display only; it does not go to the utility or a third party. The utility still obtains meter data (at hourly intervals). The HAN gateway does not preclude use of a customer-owned meter, which, as in Figure 3, separately sends meter data to a third party.
Graphics Credit: Brian P. Miller Photo & Design, http://www.brianpmillerphotography/

California IOUs will deploy embedded HAN gateways while standards for HAN communication protocols are in flux. This timing creates some risk of obsolescence. Choosing a standard that eventually loses a "standards war" could strand utility and customer investment in HAN gateways that are incompatible with HAN devices that implement the dominant standard.[144] The California IOUs have thrown their support behind the HAN communications standard ZigBee.[145] PG&E received approval to use HomePlug, which sends signals over electrical lines rather than wirelessly, to connect a fraction of its smart meters to HANs.[146]

---

[144] Standards proposed for HAN communications include ZigBee, HomePlug, 6LowPan, Bluetooth, Wi-Fi, Z-wave, among others.

[145] Troy Wolverton, *ZigBee: Household Networking Alternative to Wi-Fi and Bluetooth*, SAN JOSE MERCURY NEWS, Mar. 21, 2010, http://www.mercurynews.com/search/ci_14702782?IADID=Search-www.mercurynews.com-www.mercurynews.com&nclick_check=1 (stating that "[a]ll three major power vendors in California plan to include ZigBee radios in their meters)." Technically speaking, the ZigBee communications protocol is standardized in the ZigBee Specification.

[146] PG&E will use HomePlug in 40% of residential smart meters and ZigBee in the other 60%. CPUC, Application of Pacific Gas and Electric Company for Authority to Increase Revenue Requirements to

Sacramento Municipal Utility District (SMUD) also plans to embed a ZigBee-compliant HAN gateway in its smart meters.[147]

To address the problem of incompatible HAN communication protocols that may be adopted by utility and HAN Device manufacturers, industry participants have proposed U-SNAP (Utility Smart Network Access Port) to create a protocol-agnostic and interoperable communications standard for connecting HAN Devices to smart meters.[148] The first implementation of U-SNAP supports ZigBee, Z-Wave, RDS (Radio Data System), Wi-Fi and FlexNet;[149] and it will likely support power line standards such as HomePlug in future implementations.[150] Another solution, "Socket Interface," is recommended by the Smart Grid Interoperability Panel Home-to-Grid Domain Expert Working Group.[151] Socket Interface is "a modular appliance socket interface"[152]; USB, RS-232, and U-SNAP are all possible options for a Socket Interface.[153] The Working Group recommends that instead of embedding a specific HAN communication protocol directly inside HAN devices, manufacturers should use the generic Socket Interface, allowing customers later to choose a communications module that is compatible with their utility's infrastructure.[154]

The Smart Energy Profile 2.0 (SEP 2.0) has been identified by NIST as a standard that is applicable to HAN device communications.[155] SEP 2.0 standardizes the data model for various

---

Recover the Costs to Upgrade its SmartMeter Program 63, D.09-03-026 (Mar. 13, 2009), http://docs.cpuc.ca.gov/word_pdf/FINAL_DECISION/98486.pdf.

[147] Katie Fehrenbacher, *What to Watch For in 2010: How Utilities Will Enable ZigBee*, http://earth2tech.com/2009/12/29/what-to-watch-for-in-2010-how-utilities-will-enable-zigbee/ (last visited June 19, 2010). ("Sacramento Municipal Utility District's (SMUD) Smart Meter Project Manager Erik Krause told us via email that all SMUD smart meters will use the ZigBee wireless communication.")

[148] U-SNAP, *What is U-SNAP?*, http://usnap.org/faqs.aspx (last visited June 19, 2010). ("U-SNAP (Utility Smart Network Access Port) is a utility industry initiative whose primary objective is to create a low-cost protocol-agnostic, interoperable communications card standard for connecting HAN (Home Area Network) devices to Smart Meters.")

[149] *Id*. ("The first implementations of the U-SNAP interface support ZigBee, Z-Wave, RDS (Radio Data System), WiFi and FlexNet.?")

[150] *Id*. ("U-SNAP modules will likely support popular power line protocols such as LonWorks and HomePlug, but further investigation is required. At a minimum, there will be U-SNAP modules that bridge to popular power-line standards.")

[151] Smart Grid Interoperability Panel Home-to-Grid Domain Expert Working Group, *Free Market Choice for Appliance Physical Layer Communications*, June 4, 2010, http://collaborate.nist.gov/twiki-sggrid/pub/SmartGrid/H2G/PHY-v20.pdf.

[152] *Id.* at 2.

[153] *Id.* at 6.

[154] *Id.* at 2.

[155] NIST, *NIST Framework and Roadmap for Smart Grid Interoperability Standard, Release 1.0* 57, NIST Special Publication 1108, Jan. 2010, http://www.nist.gov/public_affairs/releases/upload/smartgrid_interoperability_final.pdf. This framework document explains that the significance of being "identified" as a standard is a "stakeholder

HAN applications based on a set of use cases. For instance, SEP 2.0 standardizes the XML format for energy usage data transmitted from smart meters to HAN devices.[156] SEP 2.0 uses IPv6 for network communications,[157] and any physical network that supports IPv6 can be used to implement SEP 2.0, such as Wi-Fi, Ethernet, ZigBee, and HomePlug.[158]

The flow of energy usage information between the HAN gateway and the customer raises issues of privacy, innovation and openness, and security. The privacy issues arise from the fact that the devices in a home area network may transmit and store sensitive information. Transmissions may be intercepted, and hackers may break into HAN devices. The primary legal protections against these threats are the criminal laws discussed in section 3.2.1. Like communications between a smart meter and a utility, those between a HAN device and a smart meter are protected from eavesdropping by federal and state anti-wiretapping laws, so long as these devices are configured to prevent them from being made available to the general public.[159] Computer fraud laws also prohibit outsiders from hacking into HAN devices that use technical mechanisms to control access. These laws, however, do not require device manufactures to provide technical protection against these threats.

Nonetheless, local routing and storage of energy usage information, such as that which could result from the HAN gateway, provides a structural constraint[160] on third-party access to energy usage information. As a result, this information flow provides one way to follow the principle of data minimization, at least as far as third-party data collection is concerned. Law enforcement access illustrates the significance of this constraint. Because we presume in this example that HAN devices are located in a customer's home, it is likely that law enforcement agents would need a search warrant either to intercept communications between a device and the smart meter or to search HAN devices for stored information.[161] Wireless signals are "electronic communications;" intercepting the contents of these communications is strictly limited by the Wiretap Act's warrant requirements.[162] HAN devices, like other objects located

---

consensus" that the standard is applicable for some Smart Grid function(s) and supports Smart Grid interoperability. *Id.* at 44.

[156] ZigBee Alliance and HomePlug Powerline Alliance, *Smart Energy Profile 2.0 Technical Requirement Document v0.5*, (Req[M-7] "the meter data structure"; Req[M-4] "simple metering data such as consumption, demand, interval data and associated measurement units shall be standardized within the profile.").

[157] *Id*. at 39 ("The Smart Energy 2.0 Profile will use IPv6 for network communications.").

[158] *Id*. at 39 ("MRD.Comm.5 -- Support all feasible physical layers (e.g., IEEE 802.15.4, 802.11, 802.39 [broadband HomePlug], forthcoming: HomePlug SE, IEEE P1901)").

[159] *See* 18 U.S.C. § 2511(2)(g) (exempting "intercept[ing] or access[ing] an electronic communication made through an electronic communication system that is configured so that such electronic communication is readily accessible to the general public" from the Wiretap Act's prohibitions).

[160] *See* Harry Surden, *Structural Rights in Privacy*, SMU LAW REVIEW, vol. 60, p. 1605 (2007).

[161] If any of this information is transmitted to and stored by a utility or third party, however, law enforcement agents would probably be able to obtain it with a lower burden process, such as subpoena or court order.

[162] *See* the discussion in section 3.1.2, above.

inside the home, are presumptively entitled to a reasonable expectation of privacy and are protected by the Fourth Amendment's warrant requirement.

The second issue that this information flow raises is the openness of the Smart Grid to customers' choices of HAN devices. The CPUC has authorized the major California IOUs to recover the costs of adding (predominantly) ZigBee-compliant HAN gateways to their meters, the degree to which device manufacturers produce ZigBee-compliant devices could have a large impact on privacy. Providing a large user base of ZigBee-enabled HAN gateways could lead to dominance of the ZigBee protocol and create an interoperability barrier to adopting devices that use other communications protocols.

Finally, the security model for the home area network carries privacy implications. In order to establish a secure communication between a utility-controlled HAN gateway and a customer's HAN device, the customer may need to register the device with the utility. We explore the privacy issues surrounding device registration in section 3.3.1.

3.2 Load Management Information Privacy Risks

Visions of the Smart Grid go beyond providing customers with timely, detailed information about their energy usage. Policymakers, utilities, and technology firms also envision providing the means to automate the control of devices to reduce demand and maintain grid stability. Enabling this control requires allowing devices to receive and respond to control messages, which we refer to as load management information. For example, the utility could send a signal to the controlling device letting it know the load is high. The controlling device could then cut the flow of electricity to an appliance or area of the home, according to a user's pre-set conditions. A user could set conditions to shut off the refrigerator for one hour a day, but ensure that another appliance or area of the home remains unaffected.

As was the case with energy usage information, load management information contains details about the in-home activities that underlie energy use. Privacy risks and legal protections, as this section illustrates, also vary with the details of how HAN devices communicate with other entities.

Enabling HAN device communications inside and outside the home also raises distinct privacy, innovation, and security issues. Device-specific data streams can reveal customer behavior more clearly than aggregate energy usage information obtained from a household. Establishing secure communications will likely require device authentication, which may, in turn, require customers to register information about their devices with utilities or other entities. This step not only exposes information about the types of devices in a house to utilities and third parties, but also raises the possibility that the device registrar will become a "gatekeeper" who can control which devices may be used on a HAN.

3.2.1 Direct Utility-HAN Device Communication

To begin, consider the relatively simple case of a utility communicating directly with HAN devices, as shown in Figure 6. Under current Smart Grid standards,[163] a utility customer must

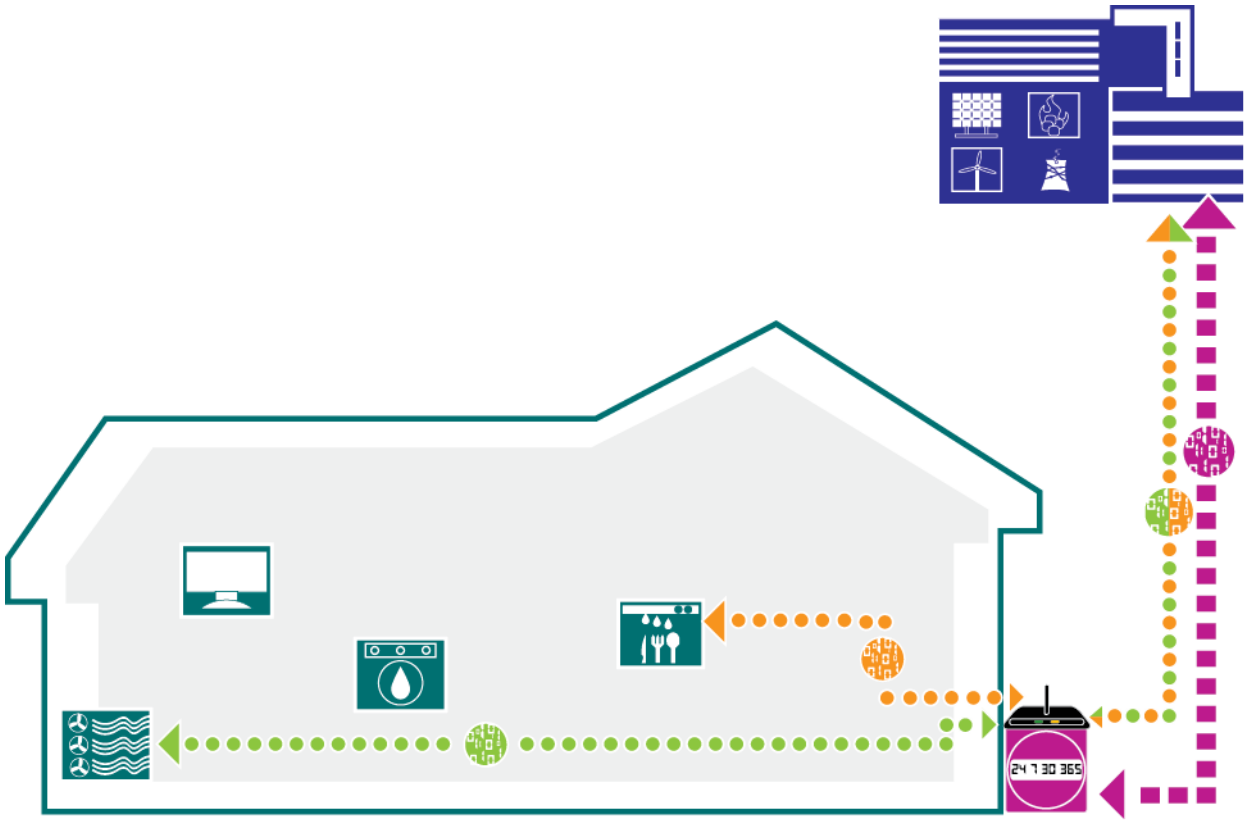
[163] As discussed in the Introduction, efforts are currently underway to standardize Smart Grid communications protocols. The description of information flow in this section is based on HAN standards identified by NIST for implementation, including Smart Energy Profile 2.0 and OpenHAN System Requirement Specification.

register a HAN device with the utility in order to establish a secure communications channel between the HAN gateway at the customer's residence and the HAN device.[164] Through the HAN gateway—note that Figure 6 shows load management information going through the HAN gateway rather than the smart meter—the utility may request and obtain the status of the registered HAN device at anytime; exchange billing demand response and load control signals with the HAN device; send pricing, messaging and billing information to the customer; and monitor and control distributed energy resources at the customer's residence. Smart Grid use cases developed by utilities envision similar information flows.[165] We defer discussion of privacy issues until the details of utility-device communications are laid out in sections 3.3.1.1-5.

[164] UCAIug OpenHAN Task Force, *UCAIug Home Area Network System Requirements Specification v1.95* at 30, "The Registration process is a further step involving Mutual Authentication and authorizing a Commissioned HAN device to exchange secure information with other Registered devices and with an ESI."

[165] *See* SCE, *2006 AMI Use Cases* and *2008-2009 Smart Grid Use Cases*, http://www.sce.com/PowerandEnvironment/smartconnect/industry-resource-center/use-cases.htm (last visited June 20, 2010); UCAIug OpenHAN Task Force, *UCAIug Home Area Network System Requirements Specification v1.95* § 4.1.

Figure 6: Utility-to-HAN load management information



Load management information (depicted as arrows composed of discrete circles) flows between the utility and the HAN gateway embedded in the smart meter. The HAN gateway routes load management information to devices inside the home. In effect, this architecture enables the utility to directly control HAN devices.
Graphics Credit: Brian P. Miller Photo & Design, http://www.brianpmillerphotography/

3.3.1.1 HAN Device Registration

In order to register a HAN device,[166] a utility customer needs to provide authentication information and detailed HAN device information to the utility.[167] The HAN device information

---

[166] The process of establishing a secure communication between a HAN gateway and a joining HAN device and enrolling the device in a utility program is given different names in different documents. *UCAIug Home Area Network System Requirements Specification v1.95* describes the process as "Commissioning, Registration, Enrollment." *Smart Energy Profile Marketing Requirements Document (MRD) v1.0* (Appendix B, section1, "Installation") uses the term "provisioning" and "registration." Here we use "registration" to refer to the entire process of establishing a secure communication between a HAN gateway and a joining HAN device and enrolling the device in a utility program. For further details see ZigBee+HomePlug Joint Working Group, *Smart Energy Profile Marketing Requirements Document (MRD) v1.0* (Appendix B, section1, "Installation") [*SEP 2.0 Marketing Requirement Document*]; SCE, *SmartConnect Use Case: C5 - Customer Uses Smart Appliances*, http://www.sce.com/NR/rdonlyres/EC46A2AC-9D43-4674-90A7-CBE47F362CDE/0/C5_Use_Case_090105.pdf (last visited June 20, 2010) [*SCE Use Case C5*].

[167] The California Energy Commission concluded in a 2008 report that "Customers have the right to receive price (periodic and real-time) signals and reliability signals without enrolling in utility programs and without registering their equipment with the utility." California Energy Commission, *Staff Report:*

may include the MAC address (a unique identifier assigned to a device by the manufacturer; MAC addresses are assigned to networkable devices like Ethernet cards and printers),[168] serial number, and device type, depending on the business practices of individual utilities.[169] This information is provided to the utility via an out-of-band mechanism (e.g., by telephone or through a website), rather than through the channel used for smart meter communications; the utility then associates the device information with the customer's account and uses it to establish secure communications through the utility-controlled HAN gateway. [170] For example, customers in Texas need to contact their Retail Electric Provider in order to add a HAN device, and they are limited to having five HAN devices connected to their smart meters.[171] (California IOUs have not yet enabled the HAN gateways in their smart meters.)

3.2.1.2 HAN Device Tracking and Monitoring

A utility may request information from a registered HAN device via the HAN gateway at any time. The types of HAN device information that the utility may request include the device manufacturer's name, model identifier, time and date code of manufacture, power source, etc.[172] In addition, the utility may request and obtain run-time status information, such as user activity and on/off frequency of HAN devices.[173]

3.2.1.3 Demand Response and Load Control (DRLC)

In a DRLC event, the utility sends DRLC signals via the HAN gateway to targeted HAN devices. The DRLC signals may include event time, duration, criticality, targeted HAN device

---

Requirements Engineering for the Advanced Metering Initiative and the Home Automation Network (AMI-HAN) Interface 4-5, Feb. 2008.

[168] MAC address stands for Medium Access Control address. *See* MAC address, MAC address, http://en.wikipedia.org/w/index.php?title=MAC_address&oldid=370775643 (last visited June 29, 2010).

[169] *SEP 2.0 Marketing Requirement Document* at 67 ("The Customer contacts the Utility/REP and gives the Utility/REP the HAN Device networking details (MAC Address, Installation Code) and the Customer account information."); *SCE Use Case C5* at 9-10 ("Customer contacts either the CSR or account manager in-person or by phone, or logs onto the utility's Web site. … [HAN device] [t]ransmits device ID, device type, and cryptographic key materials to the utility over SmartConnect network via the SmartConnect Meter.").

[170] *Id.*

[171] Smart Meter Texas, Frequently Asked Questions, https://www.smartmetertexas.com/CAP/public/home/home_faq.html#d1(last visited June 20, 2010) ("Contact your Retail Electric Provider to add HAN Devices to your account" "A Smart Meter can have up to 5 HAN Devices added." "The information about your HAN Devices is accessible by your Retail Electric Provider.").

[172] ZigBee Alliance and HomePlug Powerline Alliance, *Smart Energy Profile 2.0 Technical Requirements Document v0.5* at 71 (Req[BasicInfo-1] specifies a list of basic HAN device information and "[a]ll of the attributes shall be available via unicast requests and some [] should be available via multicast.") [*SEP 2.0 Technical Requirements Document v0.5*].

[173] *SEP 2.0 Marketing Requirements Document* at 138 ("[Utility] [s]ends a message to the HAN Device requesting the information via AMI meter [including] [c]ommunication information (e.g. log of traffic sent and received, test communication status similar to a ping of the device); [c]onfiguration information; [u]ser activity (what has been viewed and how often); On/Off frequency; [r]egistration data; HAN Device information, such as device type, model number, serial number.").

IDs or categories, load adjustment offset, and event control information. The targeted HAN device is required to provide status updates to the utility at the start and end of the DRLC event, as well as any changes to the state of the device during the event that would affect anticipated energy consumption.[174]

3.2.1.4 Pricing, Messaging, and Billing Information

In addition to DRLC information, the utility can send pricing, messaging, and billing information to registered HAN devices. Utilities may use these kinds of messages to notify customers of upcoming grid reliability events, changes in pricing, estimated bills, and energy-saving tips.[175] The utility may require the HAN devices to send back a signal to confirm the receipt of the information.[176] For instance, the utility may request a specific in-home display to confirm that that a text message has been received and displayed to a consumer.[177]

3.2.1.5 Distributed Energy Resources (DER)

The exchange of load management information can also facilitate the integration of distributed energy resource (DER), a term that refers to energy that is generated on a small scale and close to where it is used. Solar panels on a customer's house are a common example; others include small wind turbines and plug-in electric vehicles that supply electricity back to the grid.[178] A utility can monitor and control distributed energy resources on customers' premises.[179] The relevant HAN device information required for monitoring and control includes, among other things, device state (i.e., whether it is operational, on stand-by, or down for maintenance), available capacity, and power quality.[180]

3.2.1.6 Privacy Issues

The privacy issues in this case are similar to those in the smart meter-to-utility information flow discussed in Part 3.1.1. Personal and account information the customer provides to the utility are likely covered by California's security breach notification law.[181] However, the MAC address

---

[174] *SEP 2.0 Technical Requirements Document v0.5* at 47 (Req[DRLC-3], "A HAN device shall provide status updates to ESI [i.e. HAN gateway] on the start and end of a DR event, and any state changes in between the period that may affect the intended energy consumption.").

[175] *SEP 2.0 Technical Requirements Document v0.5* at 50 ("This provides the ability to notify Consumers of upcoming grid reliability events, changes in pricing (e.g., Time-of-Use period or next Inclining Block), energy tips, etc.").

[176] *SEP 2.0 Technical Requirements Document v0.5* at 51 (Req[DM-12] Report Delivery, "ESI shall support ability to send a report of message receipts to upstream systems and deliveries upon request. Delivery date/time stamps shall be sent for each device, if message required confirmation.").

[177] ZigBee Alliance and HomePlug Powerline Alliance, *Smart Energy Profile 2.0 Application Protocol Specification v0.7* at 84 ("Typically, devices which act on data obtained from servers, such as In Premises Displays or Load Controllers, will use this to indicate that a message has been obtained and acted upon, for example a TextMessage has been received and displayed to a customer.") [*SEP 2.0 Application Protocol Specification v0.7*].

[178] *SEP 2.0 Technical Requirement Document v0.5* at 65.

[179] *SEP 2.0 Technical Requirement Document v0.5* at 65 (Req[DER-1] and Req[DER-2]).

[180] *SEP 2.0 Technical Requirement Document v0.5* at 65 (Req[DER-6]).

[181] CAL. CIV. CODE § 1798.82.

and other HAN device-specific information are unlikely to fall within the definition of "personal information," so this step may not subject a utility to any regulation beyond what it faces by maintaining account information. In any event, these communications and information about them are subject to the same privacy risks (government subpoenas and warrants, hackers, and civil litigant subpoenas) and protections (FTC Act, state consumer protection laws, and federal laws against wiretapping and hacking).

The level of detail in device-specific communications, however, is qualitatively different from gross energy usage measurements, even those taken at short intervals. Device-level communications could allow utilities to develop detailed profiles about which devices customers have in their homes, where they are located in relation to each other, and how and when they use them. Though this information might allow better or more accurate load forecasting, it also creates the potential for invasive marketing campaigns that could generate consumer resistance to adoption of Smart Grid technologies.[182] This level of detail is similar to telephone calling records or Internet usage histories; all of these data types, when collected over time, can reveal a great deal about an individual's (or at least a household's) habits and activities. Yet, in contrast to phone companies and Internet service providers, which are subject to federal communications privacy laws (and, potentially, stricter state laws), utilities are subject to more varied and far less specific privacy regulations. Still, communications privacy laws do not restrict a firm's *internal* use of communications records, which leaves a major source of privacy risk unaddressed. Public utilities commissions likely have the authority to regulate these detailed information flows—including internal uses by a utility—but we are not aware of any commissions that have done so.

3.2.1.7 Choice and Innovation in Devices and Services

An architecture that *requires* customers to register their devices with utilities could also create barriers to competition in energy management services. (Privacy is one possible dimension of competition; price and quality are others.) ZigBee Smart Energy Profile 2.0 does not require the utility to register HAN devices; the technical standard instead discusses a generic "Application Trust Center."[183] Still, this *possibility* in the Smart Energy Profile 2.0 provides no guarantee that utilities will choose to communicate with Application Trust Centers that they do not control. Moreover, utilities might provide financial incentives for customers to register their devices with them, even if customers may choose other registrars. For example, SDG&E has a peak time rebate schedule in effect, which offers customers with devices that can be controlled by SDG&E a bigger discount on peak-time reductions than they would otherwise receive.[184]

---

[182] Smart Grid Interoperability Panel Home-to-Grid Domain Expert Working Group, *Free Market Choice for Appliance Physical Layer Communications*, June 4, 2010, http://collaborate.nist.gov/twiki-sggrid/pub/SmartGrid/H2G/PHY-v20.pdf ("Market tests have revealed some consumer resistance to two-way communications, particularly due to privacy concerns.").

[183] *SEP 2.0 Technical Requirements Document v0.5* at 32 (stating that "[t]he Application Trust Center is responsible for authenticating and authorizing applications" and that a customer can register with multiple Application Trust Centers as well as maintain a Center).

[184] SDG&E, Schedule Peak Time Rebate (filed Oct. 8, 2009). This schedule generally provides a $0.75 per kWh rebate for peak time reductions, but increases the rebate to $1.25/kWh for customers with "enabling technology," which is defined to mean "technology which can be initiated via a signal from the Utility

3.2.1.8 Control of HAN Devices

Finally, direct utility control over which HAN devices individuals may connect to the network is not an inevitable consequence of the Smart Grid standards we have discussed in this section. Utilities regulators exercise some control over utility investments and other business decisions that would implement (or avoid) this model. For example, the CPUC can inquire broadly into these choices under its authority to approve or reject utilities' requests to invest in AMI and to approve (dynamic) rates that take advantage of that infrastructure. The communication between a utility and a registered HAN device falls under the Commission's authority to determine "just and reasonable" electric utility rates,[185] and the CPUC has used ratemaking applications to set dynamic pricing schedules[186] and to review utilities' plans to adopt AMI components in conjunction with rate changes.[187] These proceedings have raised a number of ratepayer protection questions, such as "[h]ow to integrate effective customer education and communication with dynamic pricing tariffs"[188] and "[w]hether dynamic pricing tariffs should be voluntary, default with opt-out provisions, or mandatory."[189] Continuing attention to the details of how utilities will interact with HAN devices will help expose the privacy and control issues to public scrutiny.

3.2.2 Customer-Owned Energy Management System (EMS)

The preceding discussion presumes that customers have authorized utilities to control HAN devices. A customer may also manage HAN devices through his or her own energy management system (EMS).[190] Comparing Figures 6 and 7 illustrates the contrast. Whereas Figure 6 shows load management information going directly from the utility to HAN devices via the HAN gateway, Figure 7 introduces a customer-owned EMS to process and interpret

---

that will reduce electric energy end-use for specific electric equipment or appliances, is included in a designated Utility demand response program, and has been registered

[185] CAL. PUB. UTILS. CODE §§ 451, 454; *see also* Cal. Code Regs. tit. 20, art. 3 (setting forth CPUC's ratemaking procedures).

[186] These proceedings are separate from, but informally related to, CPUC's AMI proceeding (R.02-06-001) and utility applications that followed. *See, e.g.*, Final Opinion Authorizing Pacific Gas and Electric to Deploy Advanced Metering Infrastructure 2, CPUC A.05-06-028, July 24, 2006 (recounting this history).

[187] For example, CPUC is using PG&E's application for rate revisions to set "dynamic pricing tariffs"—a necessary step to implementing demand response—by 2011. Assigned Commissioner's Ruling and Additional Scoping Memo 8, July 25, 2006, CPUC A.06-03-005. CPUC has also reviewed utilities' requests for rate increases to recover the cost of adding or upgrading smart meters. *See, e.g.*, Decision on Pacific Gas and Electric Company's Proposed Upgrade to the SmartMeter Program 3-5, Mar. 12, 2009, CPUC D.09-03-026.

[188] Assigned Commissioner's Ruling and Additional Scoping Memo 9, July 25, 2006, CPUC A.06-03-005.

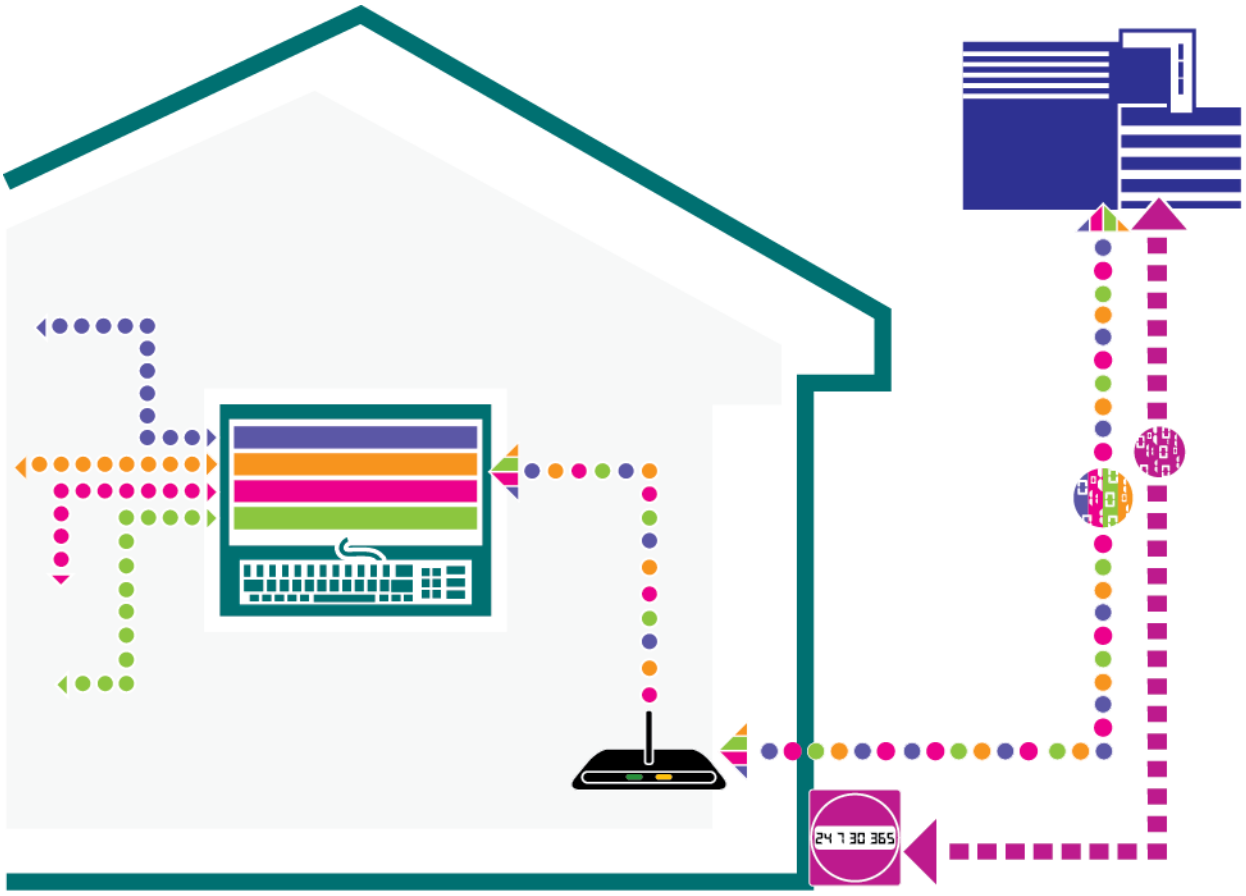
[189] *Id.* at 9. CPUC also asked whether there are "[a]ny other policy determinations that the Commission should make so that PG&E's rate design in its 2010 GRC can address dynamic pricing tariffs in a fully integrated and comprehensive manner." *Id.* at 10.

[190] UCAIug OpenHAN Task Force, *UCAIug Home Area Network System Requirements Specification v1.95* (Section 4.1.6 "Energy Management System"); *SEP 2.0 Technical Requirements Document v0.5* at 44 (Req[C-5] PEMS Proxy, "If a "Premises Energy Management System" (PEMS) is installed, to allow customization of control messages, it must register as a HAN Device for all supported function sets with the ESI, and then act as the ESI for downstream devices and handle communications as the ESI.").

commands from the utility. Under the customer-owned EMS model, the customer registers devices with the EMS and programs the EMS to respond to messages from the utility. The appliances and other HAN devices are effectively invisible to the utility, though the EMS is not.[191]

[191] SCE, *SmartConnect Use Case: C6-Customer Uses an Energy Management System (EMS) or In-Home Display (IHD)* at 18, http://www.sce.com/NR/rdonlyres/C39473B2-50BF-48C6-BAC7-4904DEE0D51F/0/C6_Use_Case_090105.pdf (last visited June 20, 2010) ("[The EMS] [e]xecutes programmed response for one or more associated HAN devices to reduce or limit load at customer's premises, based on customer preferences configured into EMS" and "[a]ssumes the customer takes responsibility for device registration with EMS and the utility has no visibility to downstream devices.").

Figure 7: Load management information flows with a customer-owned EMS



A customer-owned energy management system (EMS) (depicted as a computer keyboard and screen) routes load management information between the HAN gateway and HAN devices. The HAN gateway, in turn, routes load management information between the home and the utility. HAN devices are registered with the EMS rather than the utility.
Graphics Credit: Brian P. Miller Photo & Design, http://www.brianpmillerphotography/

The EMS market is nascent but developing rapidly. Device manufacturers have produced proof-of-concept prototypes. For instance, General Electric has introduced an energy information panel that can wirelessly connect to a smart meter and HAN devices via Wi-Fi or ZigBee in order to gather information, control devices, and recommend ways to save energy.[192] Intel introduced an Intelligent Home Energy Management Proof of Concept that can wirelessly connect a smart thermostat and appliances, and allows remote viewing and control of these

[192] General Electric, GE Smart Home-Energy Panel Tells Consumers What's Happening with Their Power Profile, http://www.gepower.com/about/press/en/2010_press/010810.htm (last visited June 20, 2010) ("The panels even will be able to be programmed to control smart appliances, thermostats and heating and cooling devices.").

devices.[193] Finally, NIST identified several EMS-related standards for implementation or further study.[194]

Compared with direct utility-HAN device communication, a customer-controlled EMS provides several privacy safeguards. First, it exposes less information about the home to the utility. Because the HAN devices are not registered with or controlled by the utility, the detailed HAN device information is invisible to the utility. If a customer-owned EMS does not route HAN communications outside the home, then utilities and third parties will not routinely have access to detailed customer usage data.[195] This is one way that a customer-controlled EMS permits more customer choice over the actions of their HAN devices in a utility event, which could produce more load response and greater customer satisfaction.[196] One potential disadvantage is that buying and maintaining an EMS may be more expensive and time-consuming than granting control of HAN devices to utilities or third parties for energy management.

The major risks to privacy come from malicious actors who may seek to intercept wireless communications or penetrate the HAN via an Internet connection. As previously discussed, encryption and other technical measures, as well as criminal laws that prohibit eavesdropping and hacking are the main forms of protection against these threats.

3.2.3 Third-Party Energy Management Systems

A third possibility for energy management is to have a third party provide the service. As shown in Figure 8, a customer could use a non-utility third party service to control HAN devices' in response to signals from utilities or the customer. These third parties may remotely administer home area networks either over the Internet or through a utility's AMI network.

Internet-based, third-party energy management services would bypass utilities. Intamac Systems, a U.K.-based company, is already offering home energy management services over broadband and cloud-computing platforms to homes in U.K. and Australia; the service goes

---

[193] Intel, *Intel Intelligent Home Energy Management Proof of Concept*, http://www.intel.com/embedded/energy/homeenergy/323157.pdf (last visited June 20, 2010).

[194] Standards related to EMS identified by NIST for implementation or further review include ZigBee Smart Energy Profile 2.0 (specifying the requirements for Premise Energy Management System), OpenHAN (including EMS use cases), IEC 61968/61970 Suites (defining application-level EMS interfaces and messaging for distribution grid management), and ISO/IEC 15067-3 (defining a model of an energy management system for the home electronic system). NIST, *NIST Framework and Roadmap for Smart Grid Interoperability Standard, Release 1.0*, at 50-73, NIST Special Publication 1108, Jan. 2010.

[195] But utilities will still have access to customer usage data measured by smart meters.

[196] CEC, *Proposed Load Management Standards (Draft Committee Report)* 27, CEC-400-2008-027-CT (Nov. 2008), http://www.energy.ca.gov/2008publications/CEC-400-2008-027/CEC-400-2008-027-CTD.PDF (last visited June 19, 2010) ("The Statewide Pricing Pilot and other similar pilots have clearly demonstrated that 'customer choice' produces significantly more load response and much greater customer satisfaction than utility control. With customer choice, the customer, not the utility, determines what loads to control, and when, if, and how much to control those loads."); E. Koch, Akuacom and M.A. Piette, *Direct versus Facility Centric Load Control for Automated Demand Response* at 7, http://drrc.lbl.gov/pubs/lbnl-2905e.pdf (last June 20, 2010) (stating that direct load control is more predictable, but an EMS has "the potential to present a more reliable response to a DR signal" because it can manage multiple resources to respond).

beyond monitoring energy usage, but controls individual devices in customer's homes via broadband.[197] Energy management companies in the U.S. are also actively working with Internet service providers to offer similar services.[198] This model might be attractive as HAN devices become popular, because it could enable customers to set the policies that their devices will follow but leave the details of administering devices to a third party.

Alternatively, a third-party energy management service provider may operate through utilities' AMI networks. There is no commercial product or service for this information flow yet, but it has been discussed in at least one utility Smart Grid use case.[199] In this information flow, a customer provides the utility with the unique identifier of the HAN device to which he or she wishes to enable third-party access and control. The utility then authenticates the customer and the third-party and, if this is successful, the utility sends the identifier to the third party. The third party may then control the HAN device through the utility's AMI network.[200] However, due to load and latency issues with utilities' AMI networks,[201] the viability of this information flow remains unclear.

The privacy risks discussed in section 3.3.1—exposing information about individual device usage and the underlying household activities—also apply to this information flow. The difference here is that public utilities commission regulatory authority is tenuous. If a non-utility energy management service provider obtains data from a utility, a commission might be able to require the utility to put privacy safeguards in contracts or service agreements with the provider. If customers send data directly to the energy management service provider, however, a utilities commission may not have, or be unwilling to exercise, jurisdiction over the provider.

---

[197] Intamac, The Dawn of Smarter Energy?, http://www2.intamac.com/blog/the-dawn-of-smarter-energy.html (last visited June 20, 2010) ("Using the Intamac web platform consumers can not only monitor the overall energy usage at their home, but control individual devices and program the service to intelligently act on their behalf.").

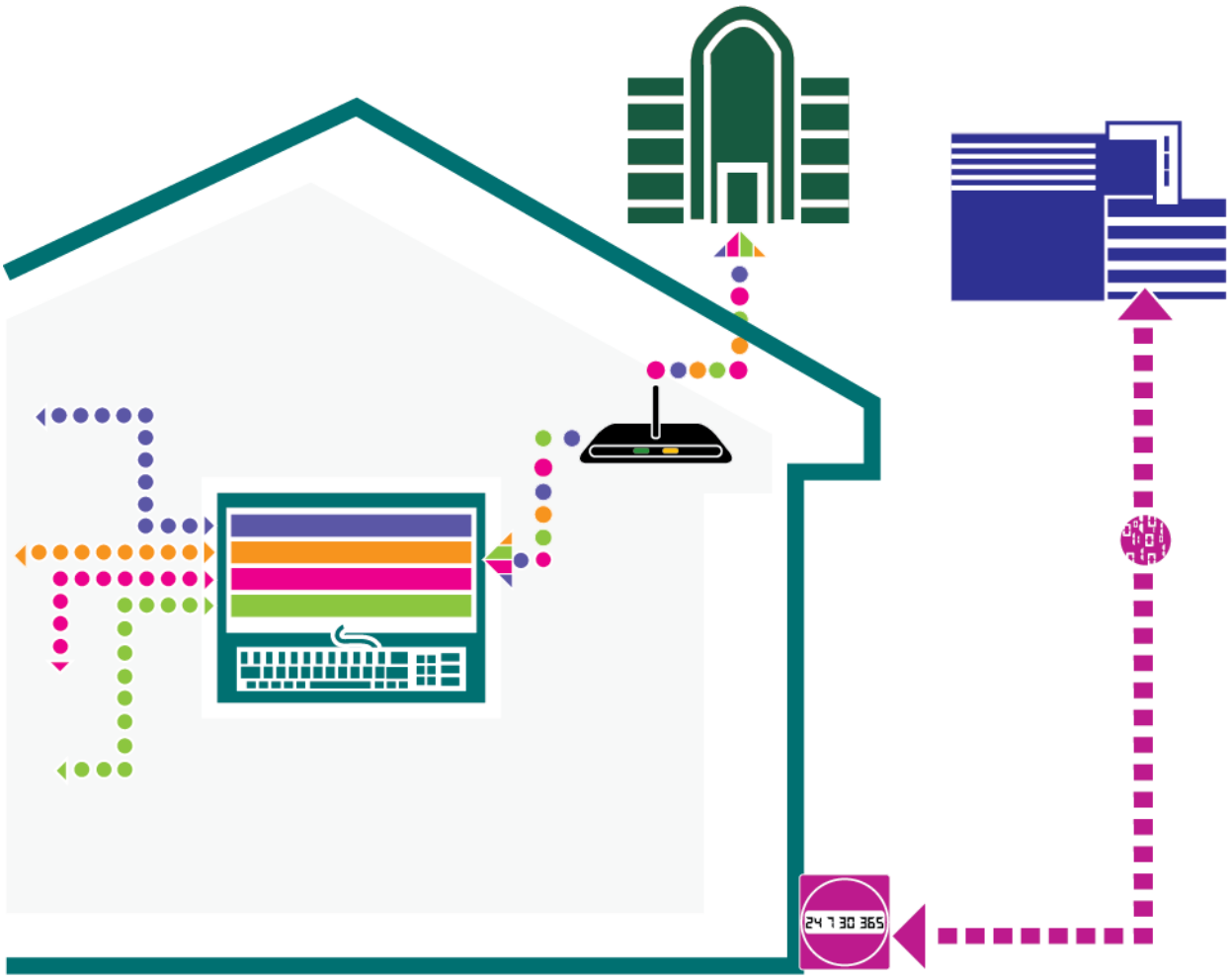
[198] Jeff St. John, Intamac Gets £4M for Home Energy Cloud Computing, http://earth2tech.com/2010/06/16/intamac-gets-4m-for-home-energy-cloud-computing/ (last visited June 20, 2010) (stating that U.S.-based such as OpenPeak and iControls are working with telecoms such as AT&T to offer energy management service over broadband); Jeff St. John, The Telco Home Energy Invasion, http://www.greentechmedia.com/articles/read/the-telco-home-energy-invasion/, (last visited June 20, 2010) (stating that Verizon and AT&T were both making moves to bring home energy platforms to their customers).

[199] SCE, AMI Use Case: C4 - External clients use the AMI to interact with devices at customer site, http://www.sce.com/NR/rdonlyres/EBE21A86-4975-48D3-AEF7-573EDDDB68D8/0/ARCHC4USECASEv13060627.pdf (last visited June 20, 2010).

[200] *Id.*

[201] Smart Grid Interoperability Panel Home-to-Grid Domain Expert Working Group, *Free Market Choice for Appliance Physical Layer Communications* at 4 (June 4, 2010), http://collaborate.nist.gov/twiki-sggrid/pub/SmartGrid/H2G/PHY-v20.pdf (last visited June 20, 2010) (explaining the load and latency problems with AMI systems when large quantities of customers participate in demand response or when real time communication is required).

Figure 8: Load management information flows with a third-party EMS



A third party administers an energy management system (EMS) for a customer. This arrangement may allow the third party to observe details about the devices in use within the home.
Graphics Credit: Brian P. Miller Photo & Design, http://www.brianpmillerphotography/

3.3 Cross-Cutting Privacy Issues in Plug-In Electric Vehicles

Plug-in electric vehicles (PEVs) combine multiple Smart Grid functions, including demand response and load control, distributed energy resource, and metering. The information flows covered in section 3.3.1 (direct utility-HAN device communications) also apply to a PEV when it is plugged in at a customer's residence.

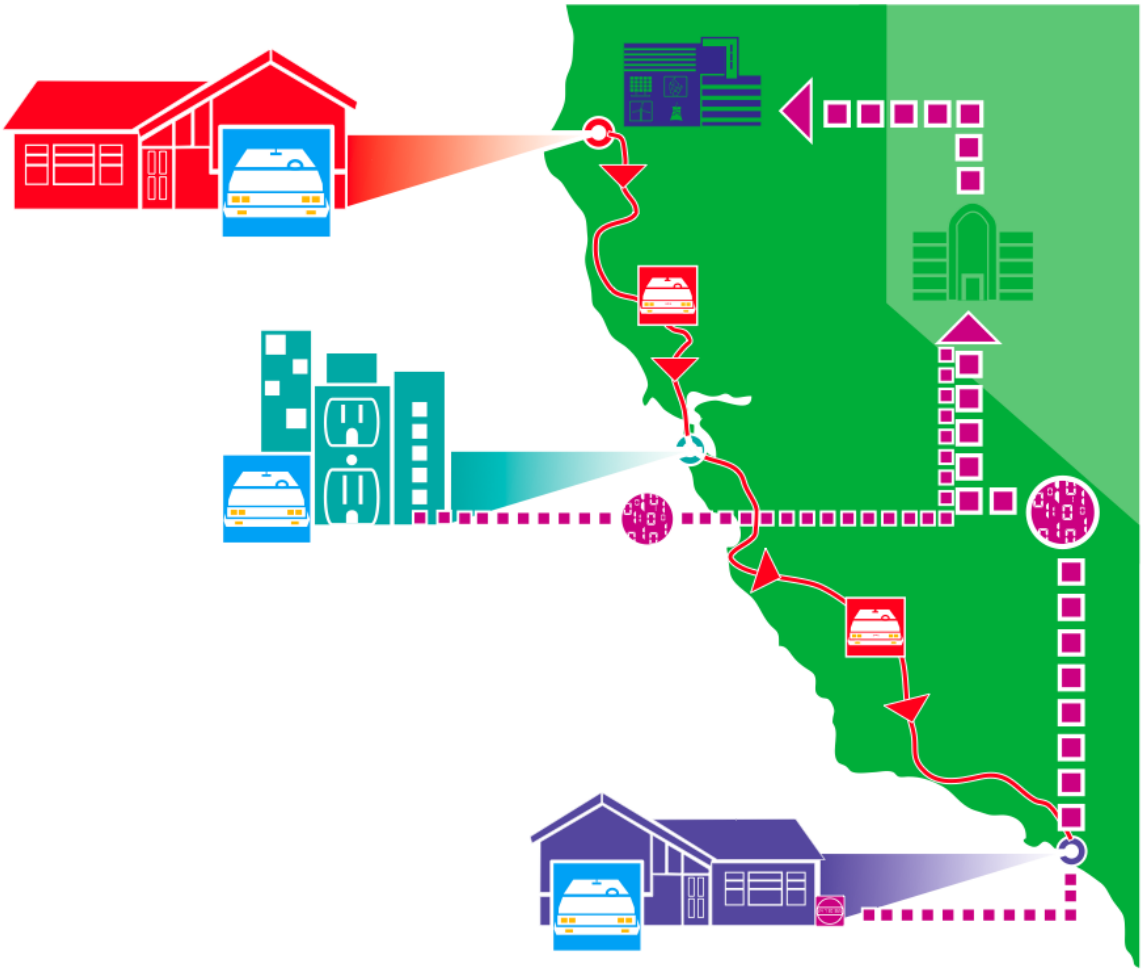
New privacy issues arise, however, when a PEV draws or supplies electricity away from a customer's residence; PEV mobility may lead to the collection of location information . As the PEV market is still nascent, this information flow is likely to evolve as PEV business models develop. Smart Energy Profile 2.0 includes a series of PEV use cases; the following discussion is based on these use cases.[202]

[202] ZigBee+HomePlug Joint Working Group, *Smart Energy Profile Marketing Requirements Document (MRD) v1.0* at 148-221 (Appendix B, section 4, "PEV Use Cases").

To enroll a PEV in utility programs, the customer contacts the utility and provides the PEV ID (e.g., the vehicle identification number), along with other authentication information of the customer. The utility authenticates the customer, and records the PEV information in its internal database.

Each time the customer charges the PEV, the PEV ID, an identifier for the charging location (named Premises ID in SEP 2.0), and other information pertaining to the electric charging session are transmitted to the utility. In order to bill the electricity charging to the proper customer account, the utility first checks PEV ID and Premises ID in its internal database. If the PEV ID and Premises ID are found, the cost is charged to the Customer's account. If the PEV ID and Premises ID are not found (i.e., the PEV is enrolled in a different utility), the PEV ID is forwarded to a clearinghouse to identify the utility that the PEV is enrolled in. The clearinghouse might store the PEV ID and Premises ID, but the current standard is unsettled as to whether the clearinghouse will store information or merely act as a channel for information exchange. If the PEV is enrolled in any utility, the cost of the charging is forwarded to the enrolled utility via the clearinghouse. Otherwise, the PEV begins charging based on the customer's selected preferences.

Figure 9. Information flows from plug-in electric vehicle charging



A plug-in electric vehicle (PEV) travels from northern to southern California. The PEV is charged along the route at a charging station and at the final destination. During both charging sessions, energy usage information is cleared through a clearinghouse in order to bill the customer for the electricity he uses to charge his vehicle.
Graphics Credit: Brian P. Miller Photo & Design, http://www.brianpmillerphotography/

PEVs introduce a privacy interest that is distinct from those discussed so far in this report: a customer's location outside the home. Location information has obvious appeal to law enforcement agencies as well as civil litigants (e.g., a spouse seeking evidence of where his or her spouse has traveled during a divorce). As with other kinds of Smart Grid data, public utilities commissions can probably create privacy rules for PEV-related data that utilities collect; but third parties are probably outside commissions' jurisdictions.

Moreover, PEV mobility means that a customer might deal with many different third parties. A customer who drives from northern to southern California (as shown in Figure 9) would begin and end his trip in different IOUs' service territory. A stop at a charging station along the way introduces a third party to the information flow. As a result, the work that the customer must do to understand how data about his location and his PEV is handled during the trip multiplies.

Travel across state lines further complicates this situation, as different states might have different privacy rules concerning PEVs. Another interstate element is the possibility that the clearinghouse for PEV information is located in a different state, as is the case in Figure 9.

Statutes that protect motor vehicle records, such as the Drivers Privacy Protection Act (DPPA)[203] and similar state laws—are unlikely to constrain either the in-state or out-of-state data flows depicted in Figure 9. The DPPA applies to disclosures of "personal information" by state motor vehicle departments, not the private parties discussed here.[204] States may extend the DPPA's baseline protections to cover more entities and more types of information, but this would leave the problem of inconsistent state protections. In the end, PEVs illustrate the need for a more comprehensive approach to Smart Grid data privacy.

[203] 18 U.S.C. § 2721 *et seq.*

[204] *See* 18 U.S.C. § 2721(a) (establishing prohibitions for a "State department of motor vehicles, and any officer, employee, or contractor thereof"); Reno v. Condon, 528 U.S. 141, 144 (2000) ("The DPPA establishes a regulatory scheme that restricts the States' ability to disclose a driver's personal information without the driver's consent.").

CHAPTER 4:
Conclusions and Recommendations

4.1 Conclusions

With vigorous state and federal support, the Smart Grid is rapidly taking shape. Although many details remain to be decided about the technical capabilities of Smart Grid components and how the Smart Grid will support broader energy policy goals in California and elsewhere, California has made a substantial investment—in terms of policy commitments and ratepayer resources—to a Smart Grid that will allow utilities to collect detailed information about residential customers' energy use, and that may allow third parties to collect far more detailed information.

This integration of information technology with the electric grid holds great potential for helping customers make better-informed decisions about their energy use. It may also serve to make the grid more reliable and resilient, reduce the growth in demand for electricity, and incorporate renewable and distributed energy sources. How utilities, regulators, and other stakeholders will make use of this data to achieve these goals is an area that deserves further exploration. Regardless, the technology and data flows pose challenges to privacy protection that require attention to the architecture and information flows of the Smart Grid as well as the adoption of new laws and policies and the expansion of those already on the books.

4.2 Recommendations

It is evident that the collection, use, and disclosure of Smart Grid data present considerable risks to individual privacy. One lesson from the rise of the commercial Internet, , as well as the integration of information technology into domains ranging from copyright[205] to healthcare, is that information practices that violate individuals' privacy expectations are likely to generate customer backlash and loss of trust. The Smart Grid is no different.

This report emphasizes that policymakers, utilities, and technology firms can adopt a systematic approach to identifying and assessing the privacy risks associated with Smart Grid deployments by analyzing information flows alongside general information privacy frameworks (e.g., FIPs) and applicable state and federal information privacy laws. Though the details of the information flows that we examined may change, and other information flow patterns will undoubtedly emerge, the approach developed in this report is adaptable to these variations.

The recommendations that we offer below are based on two overarching findings. First, the Smart Grid creates new types of data that implicate individual privacy. These data types may reveal a great deal about individual behavior but receive little or no legal protection. HAN

[205] For analysis of how rapid technological change met consumer resistance for its failure to accommodate existing legal and social norms, see Deirdre Mulligan & Aaron Burstein, *Implementing Copyright Limitations in Rights Expression Languages*, in Proceedings of the 2nd ACM Workshop on Digital Rights Management Systems (2002); Deirdre Mulligan, John Han & Aaron Burstein, *How DRM-Based Content Delivery Systems Disrupt Expectations of "Personal Use,"* in Proceedings of the 3rd ACM Workshop on Digital Rights Management Systems (2003).

device registration and communication information, location, and information associated with each charging plug-in electric vehicles are examples of Smart Grid data that may outstrip the definitions of private data under current laws and regulations.

Second, current privacy laws and regulations apply to a narrow slice of Smart Grid data and, even then, they treat different Smart Grid actors inconsistently. Some data pertaining to energy usage is clearly within the scope of established privacy law rules and regulators, while similar data collected from a different source might be subject to far less certain protection. For example, a utility and a third-party energy management service face starkly different regulatory landscapes, even though they may control and process similar data. Moreover, the laws that do protect electricity usage data generally offer lower levels of protection than privacy laws designed for data of similar sensitivity, such as telephone and Internet usage records. Establishing privacy rules that apply equally to data of similar sensitivity, irrespective of whether a utility or a third party controls the data, would help eliminate regulatory arbitrage and reduce customer confusion. Maintaining protections that are reasonably consistent with those that shielded customer privacy in the pre-Smart Grid electricity environment requires immediate action.

We recommend the following steps to help provide privacy protections that are consistent with customer expectations:

- Privacy considerations must drive architectural and information flow design decisions within the network, as well as the policies that cover Smart Grid data held by the growing array of entities that will help reap the benefit of this investment. Because privacy must be embedded in technical design, it cannot be addressed adequately by policies that created once technologies have matured.

- Because privacy risks are fairly consistent across jurisdictions, and the markets for Smart Grid technologies are national, federal policymakers should take the lead in setting legal and technical requirements to protect privacy. NIST, FERC, and the Department of Energy should recognize that the rules, standards, and guidance they develop will determine a great deal about how the Smart Grid develops. They should take advantage of this position to protect privacy.

- Recognizing that the smart grid raises privacy concerns due to the lack of consistent privacy rules for similarly situated players and the expanding amount of data they will have access to, and that federal action is unlikely to adequately address these concerns, we recommend that states act to address these gaps. State utilities regulators (such as the California Public Utilities Commission) should use their institutional expertise in protecting consumer interests and their broad authority to protect privacy through administrative rules and technical requirements. Both regulatory mechanisms have roles to play in protecting privacy.

- Privacy issues are not entirely separate from grid cybersecurity and issues of keeping the grid open to innovative devices and services. Regulators at all levels therefore should not consider them in isolation but rather use rulemakings and rate case proceedings to take the interdependencies among these issues fully into account.

- The utilities and technology firms that are building the Smart Grid should also protect privacy through their design and implementation of hardware, software, and services.

- Consumer protection and civil liberties groups should continue to engage with federal and state Smart Grid policy proceedings as well as standard-setting efforts to ensure that the technical and policy blueprints for the Smart Grid protect individual privacy.
- Widely accepted information privacy frameworks, such as the Fair Information Practices, serve as a useful starting point and should provide the foundation for all Smart Grid players to engage on privacy issues.[206]

4.3 Benefits to California

We hope that this report will be useful to technology companies, utilities, and policymakers as they identify privacy issues in the Smart Grid and reconcile privacy protections with other energy policy goals. Moreover, our approach of combining technical and legal analysis clarifies the issues that state and federal guidelines, standards, and regulations can helpfully address. We have shared elements of this report throughout its development with audiences that include policymakers, technologists, and academics. For instance, parts of this report were presented at a conference on climate change and the future of energy at the University of Toledo School of Law in March 2010 and an i4Energy Center[207] seminar at UC Berkeley in April 2010. In addition, we submitted public comments on privacy, cybersecurity, and innovation issues to the CPUC on several occasions during its Smart Grid rulemaking; and we submitted a public comment to NIST and the White House Office of Science and Technology Policy (OSTP) in response to OSTP's request for public comment on the consumer interface with the Smart Grid.[208]

[206] For a Fair Information Practice Principle based approach to Smart Grid privacy see, "Joint Comments of the Center for Democracy & Technology and the Electronic Frontier Foundation on Proposed Policies and Findings Pertaining to the Smart Grid," before the California Public Utilities Commission in the Assigned Commissioner and Administrative Law Judge's Joint Ruling Amending Scoping Memo and Inviting Comments on Proposed Policies and Findings Pertaining to the Smart Grid 33-39 (Feb. 8, 2010) (March 9, 2010).

[207] The i4Energy Center's mission is "to facilitate and promote research on system-integrated enabling technologies that will achieve better energy efficiency, improved demand/response, and dramatic improvements in energy distribution." i4Energy, Mission Statement, http://i4energy.org/mission-statement (last visited June 29, 2010).

[208] 75 Fed. Reg. 7526, Feb. 19, 2010.

GLOSSARY

Acronym/Term	Definition
AMI	Advanced metering infrastructure. A system that measures and collects customers' meter data, provides customers access to their meter data, and interfaces with smart meters and Home Area Networks at customers' residence. This infrastructure usually consists of smart meters, utility systems such as meter data management system, and a two-way communication network between utility systems and customers' residences.
Customer	An individual who has a privacy interest in data about energy usage at a residence. This report uses "customer" to refer to a residential customer, unless otherwise noted.
Demand response	Changes in energy usage by customers from their normal usage patterns in response to changes in electricity price, incentive payments, or systems reliability signals.
DER	Distributed energy resource: Small, modular, energy generation and storage technologies that provide electric capacity or energy where it is needed.[209] Examples of DER include solar panels, small wind turbines, and plug-in electric vehicles that supply electricity back to the grid.
DRLC	Demand response and load control
ESP	Electric Service Provider: Non-utility entity that offers electric service to customers within the service territory of an electric utility.[210]
EMS	Energy Management System: An application used for controlling multiple HAN devices according to a customer's preference. It may be a stand-alone device, but it may also reside in HAN devices such as Programmable Communicating Thermostats, In-Home Displays, etc.
Energy Service Interface	See HAN gateway.
Energy usage information	Energy usage information includes price information, consumption and time-of-use information.
HAN	Home Area Network: A network at a customer's residence used for communicating with the customer's devices for Smart Grid-related functions.
HAN device	Home Area Network device: A device that can communicate on the HAN. A "smart appliance" or a "smart device" is a HAN device that can communicate over the HAN and adjust its behavior. This report does not distinguish a HAN device and a smart appliances/device, but refer to them generally as a "HAN device."

[209] Definition of DER provided by the Department of Energy, http://www1.eere.energy.gov/femp/pdfs/31570.pdf (last visited June 21, 2010).

[210] Definition of ESP provided by the California Public Utilities Commission, http://docs.cpuc.ca.gov/published/ESP_lists/esp_udc.htm (last visited June 21, 2010).

HAN gateway	Home Area Network gateway: A gateway device through which a customer's HAN communicates with the customer's utility or any other entity that provides energy management services. A customer may have multiple HAN gateways on the customer's premise, and the same HAN device may communicate with multiple HAN gateways. Although HAN gateways are embedded in smart meters by major California utilities, HAN gateways and smart meters are logically separate; a HAN gateway can be a stand-alone device, integrated with a HAN device, or embedded in a smart meter. The HAN gateway is also known as Energy Service Interface (ESI).
IOU	Investor-owned utility. See Utility
Load management information	Load management information includes price and event signals from utilities, control traffic exchanged among HAN devices and the systems and entities that control them, and HAN device identification and authentication information.
MAC address	Media access control address: A unique identifier for a network interface device. For example, Ethernet interfaces have 48-bit MAC addresses.
Meter data	Any data collected by an electric meter, such as the consumption and time-of-use information, quality of service data, communications configurations, and security-related data. If HAN gateways are embedded in smart meters, meter data only refers to the data associated with metering function of the smart meters, excluding the data associated with HAN function of the smart meters.
Smart appliance/device	See HAN device.
SEP 2.0	Smart Energy Profile 2.0: A standard developed by ZigBee Alliance and HomePlug PowerLine Alliance that defines communications and information model for HAN devices. It has been identified by National Institute of Standards and Technology as one of the Smart Grid standards for implementation.
Use case	Description of the interaction of different actors (customers, utilities, and others), and the functional requirements to implement these interactions within the Smart Grid.
POU	Publicly owned utility. See Utility.
Utility	In this report a utility refers to a vertically integrated utility from the perspective of residential customers in California. This report does not consider the different types of service providers in a restructured retail electricity market. Based on types of ownership, utilities are categorized into investor-owned utility (IOU), publicly owned utility (POU), and cooperative utility. The IOUs are private corporations; the authority of state Public Utility Commission (PUCs) is often limited to the IOUs. POUs are owned by municipal, state, or federal governments; POUs are self-

	regulated by their governing boards and are generally not subject to state or federal economic regulation.

APPENDIX A:

CPUC Decisions Approving Residential AMI Investments

This table is compiled from the CEC's *Proposed Load Management Standards (Draft Committee Report)*[211] , CPUC decisions approving IOUs' AMI investments,[212] and utility website.[213]

	PG&E		SDG&E	SCE
CPUC decision	D. 06-07-027 (original plan in 2006)	D. 09-03-026 (update in 2009)	D. 07-04-043	D. 08-09-039
Communication network	PLC for its electric; RF for gas	RF mesh	RF mesh	RF mesh
Customer access to meter data	Internet Access	Internet access + HAN	Internet access + HAN	Internet access + HAN
15-minute data for commercial and industrial customers	Yes	Yes	Yes	Yes
Hourly data for residential customers	Yes	Yes	Yes	Yes
Two-way communication	Yes	Yes	Yes	Yes
Remote updatability	No	Yes	Yes	Yes

[211] Calif. Energy Comm'n, *Proposed Load Management Standards (Draft Committee Report)* 27, CEC-400-2008-027-CT (Nov. 2008), http://www.energy.ca.gov/2008publications/CEC-400-2008-027/CEC-400-2008-027-CTD.PDF (last visited June 19, 2010). See in particular pp. 23-25 (summarizing AMI implementation as of November 2008).

[212] CPUC Decision 09-03-026 (HAN gateway in PG&E Smart Meter has both ZigBee and HomePlug connection); CPUC, *Demand Response and Advanced Metering*, http://www.cpuc.ca.gov/PUC/energy/Demand+Response/R0206001.htm (last visited June 20, 2010) (list of decisions approving IOUs' deployment plans).

[213] PG&E, *New Technologies*, http://www.pge.com/about/news/mediarelations/newsimages/newtech/ (last visited June 20, 2010) (PG&E employs RF Mesh network).

Physical interface of HAN Gateway	No	ZigBee and HomePlug	ZigBee	ZigBee

APPENDIX B:

Major HAN Communication Protocols

The features of these HAN communication protocols can be summarized in the table below:[214]

Protocol	**Wired/Wireless**	**One/Two way**	**Openness**
ZigBee	Wireless	Two way	Private, available to license holders.
HomePlug	Wired, power line communication	Two way	Private, available to license holders.
6LowPan	Wireless	Two way	IETF standard
Bluetooth	Wireless	Two way	IEEE standard
Wi-Fi	Wireless	Two way	IEEE standard
Z-wave	Wireless	Two way	Private, available to license holders.

[214] Charles McParland, *Home Network Technologies and Automating Demand Response* at 19, http://drrc.lbl.gov/pubs/lbnl-3093e.pdf (last visited June 20, 2010).